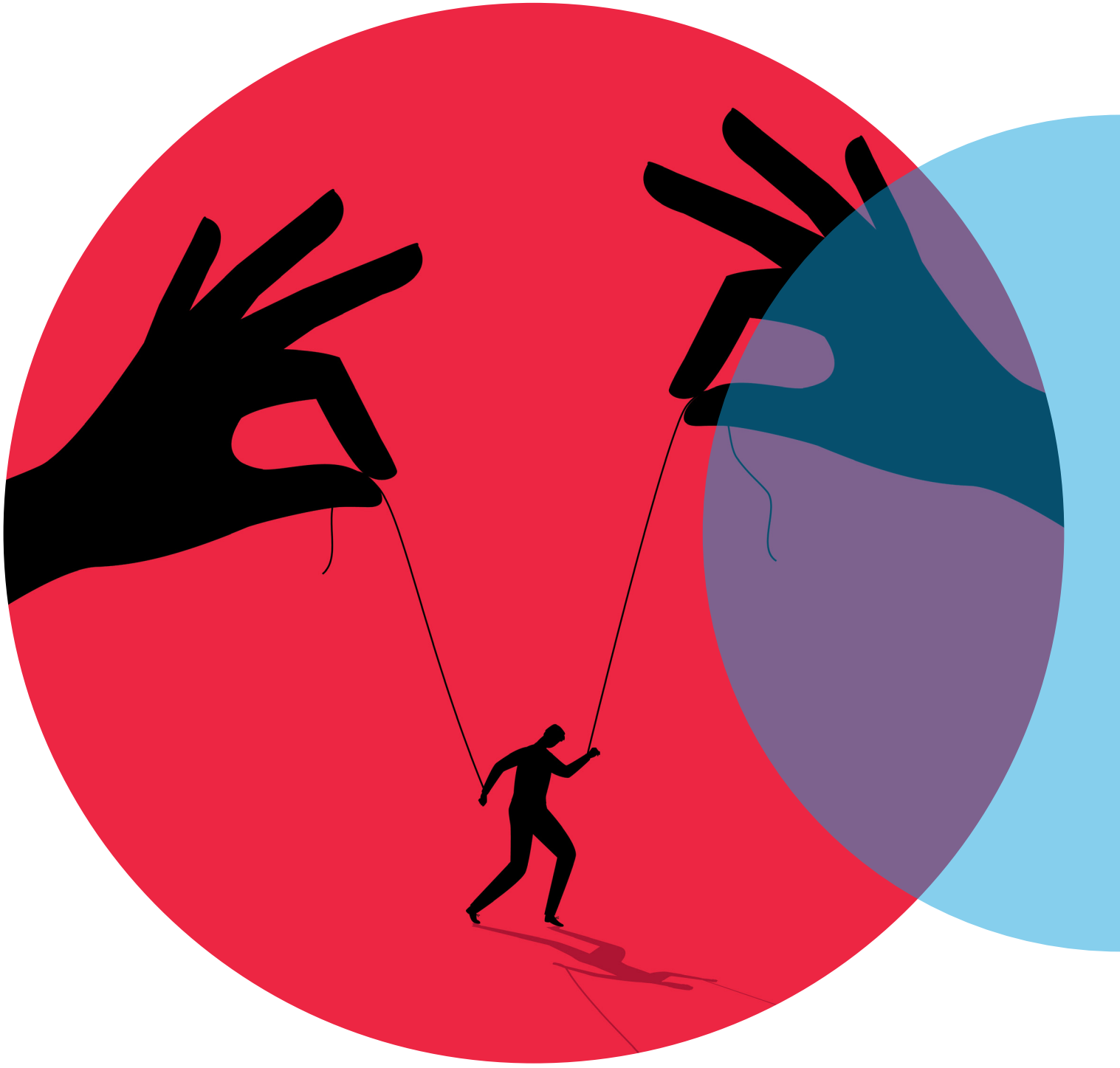
Hybrid CoE Paper 27

Handbook on the role of non-state actors in Russian hybrid threats



Hybrid CoE

Eginhards Volāns, Vladimir Rauta, Magda Long, Andis Kudors, Agata Kleczkowska and Eliza Lockhart – December 2025

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

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

ISBN 978–952–7591–30–7 (web)
ISBN 978–952–7591–31–4 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

December 2025

Cover photo: StockSmartStart / Shutterstock.com

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is an autonomous, network-based international expert organization dedicated to addressing hybrid threats. Hybrid CoE's mission is to enhance the security of its 36 Participating States, the European Union, and NATO by providing expertise, training, and networks to counter hybrid threats. Its core values are excellence, integrity, and respect. The Centre is located in Helsinki, Finland.

Contents

Key takeaways

- Non-state actors (NSAs) are central to Russia's "grey zone" strategy, allowing the Kremlin to project power while maintaining deniability. The use of NSAs is embedded in Russia's strategic culture, rooted in the Soviet era and the practices of the KGB.

- NSAs can be effective in various conditions, ranging from peacetime to hybrid threats and from hybrid to conventional warfare. Russia has long used NSAs to influence its own population and allies, destabilise adversaries, and even fight enemies on the battlefield.

- Relationships between NSAs and the Russian government are complex, informal, and fluid, often driven by profit, ideology, or both. Nevertheless, there are strong indications of state involvement. At the same time, the coherence and coordination of these activities should not be overstated, as the decision-making process in Russia can often be fragmented and ad hoc.

- Most NSAs maintain ties to several key state institutions, most notably the Presidential Administration, which serves as a strategic hub for planning, decision-making, and coordination, as well as Russian intelligence services, which are directly involved in the practical orchestration of NSAs.

- The Russian regime's reliance on NSAs, and their reliance on the regime, has likely increased since the invasion of Ukraine, as direct activities by the Russian state have faced increased exposure and countermeasures.

- The NSAs most frequently used by Russia are diverse and often have overlapping roles. They can operate in various domains simultaneously, in a fluid and adaptable manner, rather than in strictly defined silos. Nevertheless, distinct categories with shared characteristics can be identified.

- Armed NSAs form a fluid ecosystem where state and non-state, legal and illegal forces overlap. They serve as enforcers, disruptors, and emissaries of influence for the Kremlin, providing deniability and operational flexibility. Their clandestine and volatile ties to security forces, industry giants, and political elites make attribution to the Russian regime difficult.

- Cyber NSAs are employed for espionage, disruption, and for providing support in information operations. While the backbone of Russia's offensive cyber programme still lies within state-controlled hacking groups, since 2022 hacktivists and cybercriminals have been used increasingly. Russia's offensive cyber programme also relies on various enablers, such as research institutes and IT companies, which are necessary for the development of Russia's offensive cyber capabilities.

- Propaganda and disinformation NSAs are a cost-effective tool in Russia's hybrid threat toolbox. Their activities are increasingly outsourced to private entities but remain under tight state control. More unconventional and apolitical actors, including social media platforms, influencers, and cultural figures, are increasingly being used to shape narratives in Russia and abroad.

- Social and political NSAs are used to project Russia's sharp power and to influence foreign legislative processes in its favour. They exploit traditional values, falsify history, work closely with the Russian compatriot community, and, more recently, have stepped up their activities in developing countries.

- Economic and financial NSAs play a crucial role in Russia's ability to exert economic and financial influence abroad. However, their international reach has been hindered by Western sanctions, resulting in a more inward focus. As sanctions have intensified, these actors, along with others, have been mobilised to evade them.

List of abbreviations

ANSA – Armed Non-State Actor
APT – Advanced Persistent Threat
CAR – Central African Republic
CARR – Cyber Army of Russia Reborn
CBR – Central Bank of Russia
CIS – Commonwealth of Independent States
CNSA – Cyber Non-State Actor
DShRG – Sabotage Assault Reconnaissance Group
EFIS – Estonian Foreign Intelligence Service
EFNSA – Economic and Financial Non-State Actor
ERA – European Russian Alliance
EU – European Union
FCRB – First Czech Russian Bank
FSB – Federal Security Service of the Russian Federation
GRU – Main Directorate of the General Staff of the Armed Forces of the Russian Federation
HMF – Historical Memory Foundation
HRAGIF – Human Rights Accountability Global Initiative Foundation
Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats
IACP – International Agency for Current Policy
IDC – Russian Institute for Democracy and Cooperation
IT – Information Technology
KAPO – Estonian Internal Security Service
KGB – Committee for State Security of the USSR
LCK – Latvian Human Rights Committee
MFA – Ministry of Foreign Affairs of the Russian Federation
MoC – Ministry of Culture
MoD – Ministry of Defence of the Russian Federation
MoF – Ministry of Finance of the Russian Federation
NATO – North Atlantic Treaty Organisation
NGO – Non-Governmental Organisation
NMG – National Media Group
NPO – Non-Profit Organisation
NSA – Non-State Actor
OMON – Special Purpose Mobile Unit
PA – Presidential Administration of the Russian Federation
PDNSA – Propaganda and Disinformation Non-State Actor

PMC – Private Military Company
PR – Public Relations
Pravfond – Foundation for the Support and Protection of the Rights of Compatriots Living Abroad
RCC – Russian Congress of Canada
RDIF – Russian Direct Investment Fund
RIS – Russian Intelligence Services
RIM – Russian Imperial Movement
RISI – Russian Institute for Strategic Studies
ROC – Russian Orthodox Church
Rosgvardiya – National Guard of the Russian Federation
Rossotrudnichestvo – Federal Agency for the Commonwealth of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation
RUSI – Royal United Services Institute
SDA – Social Design Agency
SOBR – Special Rapid Response Unit
SOC – Serbian Orthodox Church
SPNSA – Social and Political Non-State Actor
SSS – Sewa Security Services
SVR – Foreign Intelligence Service of the Russian Federation
TAC – Legal Protection Centre
TCN – Transnational Crime Network
Voenkory – War correspondents

Introduction

By Vladimir Rauta

Whether through attacks on German military and industrial facilities by individuals,[1] sabotage of French rail infrastructure by loosely co-ordinated groups,[2] disinformation campaigns run by private companies,[3] or cyber operations by hacktivist collectives,[4] **Russia's employment of non-state actors (NSAs) is a staple of its approach to hybrid threat operations.**

This handbook seeks to provide an overarching assessment of Russia's approach to working with and through various NSAs across different operational domains, mapping both the empirical depth and breadth of the phenomenon. It establishes a much-needed baseline for understanding the logic behind Russia's employment of NSAs and lays the groundwork for determining appropriate measures and countermeasures at a time when operations below and above the threshold of war are on the rise.

The handbook is designed for practitioners and readers who may not have prior in-depth knowledge but who require a clear and accessible introduction to the topic.

It asks how and why Russia uses NSAs and, in doing so, touches on several related policy questions:

- Is there a grand strategic approach to Russia's employment of NSAs?
- How do NSAs orchestrated by Russia differ typologically?
- Are all NSAs orchestrated by Russia proxies?
- What is their strategic utility across operational domains?
- How have these NSAs and their relationship to the Russian state evolved?

The handbook focuses on five categories of NSAs distinguished by their domain of operation:

- Armed non-state actors.
- Cyber non-state actors
- Propaganda and disinformation non-state actors
- Social and political non-state actors
- Economic and financial non-state actors

Each category of NSA is discussed in turn and analysed within the context of Russia's broader strategy, examining the practices, logics and rationales behind the use of NSAs, their relationship to the Russian regime, and their purpose and role in hybrid threats. The use of NSAs in Russian hybrid threat operations is exemplified by recent case studies that focus on, but are not limited to, Hybrid CoE's Participating States or regions where their interests are threatened.[5] The handbook also

1 Kate Connolly, 'Germany Arrests Two Dual Nationals on Suspicion of Plotting Attacks for Russia', The Guardian, 18 April 2024, https://www.theguardian.com/world/2024/apr/18/germany-arrests-two-for-alleged-plot-to-attack-military-bases-on-behalf-of-russia.

2 Ivana Kottasová, Saskya Vandoorne, and Sana Noor Haq, 'Who Was Behind the Sabotage of France's Railway Network? Here's What We Know', CNN, 27 July 2024, https://edition.cnn.com/2024/07/27/europe/france-train-attacks-explainer-2024-paris-olympics-intl/index.html.

3 'What Is the Doppelganger Operation? List of Resources', EU DisinfoLab, 15 May 2025, https://www.disinfo.eu/doppelganger-operation/.

4 'Poland Says Russian Cyberspies Targeted Government Networks', Reuters, 8 May 2024, https://www.reuters.com/technology/cybersecurity/poland-says-it-was-targeted-by-hacking-attack-russia-linked-group-apt28–2024–05–08/.

5 As of June 2024, Hybrid CoE's Participating States include all EU and NATO members.

identifies key Russian state institutions that orchestrate NSAs in hybrid threats. It culminates in conclusions and knowledge gaps that point to areas for further research.

This analysis incorporates Hybrid CoE's established vocabulary and employs the term "non-state actor" as defined in *The Landscape of Hybrid Threats: A Conceptual Model*, a landmark conceptual document jointly developed by the European Commission's Joint Research Centre (JRC) and Hybrid CoE. NSAs are defined therein as "entities that play a part in international relations and that exercise sufficient power to interfere, influence and cause change without any affiliation to the established institutions of a state"[6] and as ranging "from individuals to private corporations, religious institutions, humanitarian organisations, armed groups and de facto regimes in actual control of territory and population".[7]

6 Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou, 'The Landscape of Hybrid Threats: A Conceptual Model' (The European Commission and Hybrid CoE, November 2020), 22, https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf.

7 Janne Jokinen, Magnus Normark, and Michael Fredholm, 'Hybrid Threats from Non-State Actors: A Taxonomy', Hybrid CoE Research Report 6 (Hybrid CoE, June 2022), 6.

The complexity of non-state actors in hybrid threats

By Vladimir Rauta

Russia's hybrid threat and hybrid warfare strategies[8] combine a diverse range of kinetic and non-kinetic means, including physical attacks on infrastructure; disinformation and propaganda; assassinations; cyberattacks; and even the fomenting of *coups d'état* or secessionist insurgencies through armed proxies. Such operations have been pursued across the full spectrum of military and non-military domains by an ever-expanding mix of state and non-state actors. For Russia, these operations form part of a strategy of placing small bets designed to "square [the] circle of maximal ambitions and weak conventional capabilities".[9]

Russian hybrid threats are often seen as ambiguous because they involve many operations short of war. This perception often stems from the difficulty of analysing the complex relationships between the Russian state and the NSAs it employs. Furthermore, not all NSAs are used in hybrid threats or act as Russian proxies. As a result, the issue is complex to analyse and undermines the development of effective countermeasure strategies.

This section evaluates two features of NSAs that illustrate how Russia employs and engages with them, helping to explain the reasoning behind their use in hybrid threats:

- NSA typological diversity
- State–NSA relational variation

The notion of NSA lacks a universal definition.[10] It serves as an umbrella term covering a multitude of entities, broadly characterised by their independent existence vis-à-vis sovereign states. NSAs are, therefore, diverse by the very nature of the many actors that fall under this label. NSA typological diversity is evident in Russian hybrid threats in the Baltic–Nordic region, where individuals commit various forms of vandalism against historical monuments;[11] commercial entities purchase strategically located island and coastal properties;[12] the Russian Orthodox Church (ROC) finances construction projects near sites of national security importance; or Russia's so-called shadow fleet circumvents sanctions on oil exports.[13]

8 In Russian strategic thinking, such activities have been described as 'complex approaches' and 'new generation war'. See Andrew E. Kramer, 'Russian General Pitches "Information" Operations as a Form of War', The New York Times, 2 March 2019, https://www.nytimes.com/2019/03/02/world/europe/russia-hybrid-war-gerasimov.html.

9 Daniel Byman and Seth G. Jones, 'Russia's Grey Zone Threat After Ukraine', The National Interest, 29 September 2023, https://nationalinterest.org/feature/russias-gray-zone-threat-after-ukraine-206837.

10 Agata Kleczkowska, 'States vs non-state actors – A public international law perspective', Strategic Analysis No. 20 (The European Centre of Excellence for Countering Hybrid Threats, January 2020), https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-20-states-vs-non-state-actors-a-public-international-law-perspective/.

11 'Act of Vandalism Against Monument to Freedom Fighter May Be Related to 9 May', Delfi, 8 May 2023, https://www.delfi.lt/en/politics/act-of-vandalism-against-monument-to-freedom-fighter-may-be-related-to-9-may-93287943.

12 Andrew Higgins, 'Mystery Island in Finland', The New York Times, 3 November 2018.

13 Minna Ålander and Patrick Oksanen (eds.), 'Tracking the Russian Hybrid Warfare: Cases from Nordic-Baltic Countries' (Stockholm Free World Forum, n.d.), https://frivarld.se/rapporter/tracking-the-russian-hybrid-warfare-cases-from-nordic-baltic-countries/.

This handbook focuses on five categories of NSAs frequently used in Russian hybrid threats:

- **Armed NSAs** (ANSAs) include private military companies (PMCs), transnational criminal networks (TCNs), paramilitary formations, militias, terrorist groups, contract killers, and disposable agents.
- **Cyber NSAs** (CNSAs) range from state-controlled hacking groups to hacktivists, cybercriminals, and cyber enablers such as IT companies and research centres.
- **Propaganda and disinformation NSAs** (PDNSAs) include traditional media, digital media, influencers, culture and arts actors, and propaganda and disinformation enablers such as PR agencies.
- **Social and political NSAs** (SPNSAs) comprise think tanks, compatriots, sharp power,[14] history-linked organisations, as well as the ROC, political parties and lobbyists.
- **Economic and financial NSAs** (EFNSAs) refer to the role played by oligarchs, state-aligned corporations, and sanctions-evasion enablers, often outsourced from other categories of NSAs.

The advantage of this typological assessment lies in its ability to map the breadth of Russia's use of diverse NSAs, improving our understanding of the complex Russian hybrid threat landscape.

The diversity of NSAs corresponds to the variation in their relationships with state sponsors. In short, just as not all NSAs are the same, not all state–NSA relationships are alike. In the Russian context, most examples are characterised as proxy relationships. While some NSAs are indeed proxies, others are better described as auxiliaries, affiliates or surrogates. Although different types of state–NSA relationships can be identified, it is often challenging to fit them neatly into categories, as information on the underlying relationship dynamics is typically very limited. State–NSA relationship types are described in detail in Hybrid CoE's key study, *Hybrid Threats from Non-State Actors: A Taxonomy*.[15]

Russia's reliance on NSAs in hybrid threats follows the familiar logic of conflict delegation. This refers to "a strategy in which a foreign government commits material resources or military expertise to a non-state armed group to target a perceived adversary".[16] Although typically associated with armed groups, the logic of conflict delegation applies to non-armed actors as well. The use of NSAs is cost-effective, deniable, and risk averse. It is not surprising, therefore, that using NSAs has been labelled

14 Sharp power refers to efforts by authoritarian regimes to penetrate and manipulate vulnerable democracies through media, academic, cultural, and think-tank initiatives that distort or influence public perception. Christopher Walker and Jessica Ludwig (eds.), 'Sharp Power: Rising Authoritarian Influence', International Forum for Democratic Studies Report (National Endowment for Democracy, December 2017), https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

15 'Hybrid Threats from Non-State Actors', 11.

16 Niklas Karlén, Vladimir Rauta, Idean Salehyan, Andrew Mumford, Belgin San-Akca, Alexandra Stark, Michel Wyss, Assaf Moghadam, Allard Duursma, Henning Tamm, Erin K. Jenne, Milos Popovic, David S. Siroky, Vanessa Meier, Alexandra Chinchilla, Kit Rickard, and Giuseppe Spatafora, 'Forum: Conflict Delegation in Civil Wars', *International Studies Review*, Volume 23, Issue 4 (2021): 2048–2078, 2051.

both "the least bad option"[17] and "a superficially seductive policy option".[18]

The characterisation of NSAs as Russian proxies, however, is difficult in practice, not least because "grey zone" activities thrive on ambiguity and the often-cited blurring of peace and war.[19] This creates an asymmetric playing field in which Russia delegates to NSAs a range of subversive activities that accomplish the desired strategic goals at low cost while providing the strategic benefits of plausible deniability.[20] Some scholars have argued that deniability is hardly bulletproof given how easily and frequently sponsorship can be identified,[21] while others contend that a more accurate concept is, perhaps, that of implausible deniability.[22] As was recently pointed out in an essay on maritime sabotage, the act of naming and shaming is unlikely to deter future attacks by itself.[23]

17 Tyrone L. Groh, *Proxy War: The Least Bad Option* (Stanford University Press, 2019).
18 Geraint Alun Hughes, 'Syria and the Perils of Proxy Warfare', *Small Wars & Insurgencies*, Volume 25, Issue 3 (2014): 522–538, 523.
19 Silvie Janičatová and Petra Mlejnková, 'The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political–Military Discourse on Russia's Hostile Activities', *Contemporary Security Policy*, Volume 42, Issue 3 (2021): 312–344; Chiara Libiseller and Lukas Milevski, 'War and Peace: Reaffirming the Distinction', *Survival: Global Politics and Strategy*, Volume 63, Issue 1 (2021): 101–112.
20 Karlén et al., 'Forum: Conflict Delegation in Civil Wars'.
21 David Blagden, 'Deterring Cyber Coercion: The Exaggerated Problem of Attribution', *Survival: Global Politics and Strategy*, Volume 62, Issue 1 (2020): 131–148.
22 Rory Cormac and Richard J. Aldrich, 'Grey is the New Black: Covert Action and Implausible Deniability', *International Affairs*, Volume 94, Issue 3 (2018): 477–494.
23 Walker D. Mills, 'Maritime Sabotage: Protecting Europe's Soft Underbelly', Irregular Warfare Initiative, 19 March 2023, https://irregularwarfare.org/articles/maritime-sabotaging-protecting-europes-soft-underbelly/.

Non-state actors, hybrid threats and international law

By Agata Kleczkowska

At the core of these dilemmas lie issues of attribution, best framed by asking whether it is possible to hold Russia responsible for certain actions under the international legal framework. According to the Articles on Responsibility of States for Internationally Wrongful Acts, to establish that a state has committed an internationally wrongful act, the conduct in question has to be attributable to the state under international law and must constitute a breach of one of its international obligations.[24] Thus, to hold Russia responsible, the actions of the NSAs described below must first be attributed to it.

The conduct of an NSA could be considered an act of a state under international law if the NSA was acting on the instructions of, or under the direction or control of, that state.[25] This standard is often associated with the **effective control test**, described in the *Military and Paramilitary Activities in and Against Nicaragua* case, in which the International Court of Justice held that a state's general control over a highly dependent NSA was not sufficient for attribution, as the state must exercise effective control over the NSA's actions.[26] **The threshold for attribution is therefore very high: a state must give instructions to the NSA concerning each specific wrongful act or exercise effective control over each such act.**

The effective control test is not, however, the only standard of attribution. The International Criminal Tribunal for the former Yugoslavia presented the so-called **overall control test** in the *Prosecutor v. Duško Tadić* case. Under this test, to attribute an NSA's actions to a state, it must be shown that the state has overall control over the group, not just by funding and equipping it, but also by coordinating or planning its activities. However, the state does not need to give direct orders for specific illegal acts to the group's leadership or members.[27]

Both tests have their proponents and opponents.[28] Until the dilemma between them is resolved, states will be able to exploit the "grey zone" that exists within the rules of international responsibility to conceal their involvement in the actions of NSAs.

24 Article 2, International Law Commission, 'Responsibility of States for Internationally Wrongful Acts', Yearbook of the International Law Commission, Volume 2, Part Two (2001), https://legal.un.org/ilc/publications/yearbooks/english/ilc_2001_v2_p2.pdf.

25 Article 8, ibid.

26 Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) (Merits), ICJ Reports 14 (1986), para. 115, https://www.icj-cij.org/sites/default/files/case-related/70/070–19860627-JUD-01–00-EN.pdf.

27 Prosecutor v. Duško Tadić, Appeals Chamber, Judgment, IT-94–1-A, 15 July 1999, para. 131.

28 See Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) (Merits), ICJ Reports 43 (2007), para. 404– 406; Stefan Talmon, 'The Responsibility of Outside Powers for Acts of Secessionist Entities', *International and Comparative Law Quarterly* 58 (2009): 517; Marko Milanovic, 'State Responsibility for Genocide', *European Journal of International Law* 17 (2006): 577– 581, 584– 585; Michael N. Schmitt and Liis Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution', *Fletcher Security Review* 1 (2014): 64; 'Report: The Legal Framework Regulating Proxy Warfare' (American Bar Association, Center for Human Rights & Rule of Law Initiative, December 2019), 15; International Committee of the Red Cross, 'Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Commentary of 2016', para. 271, https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949/article-2/commentary/2016.

Secondly, the action attributed to the state must be recognised as a violation of international law. There are no international legal norms specifically tailored to address many of the actions described in this report; this is true, for example, of disinformation, covert influence on legal processes, election meddling, or attacks on critical infrastructure. Some of these may amount to violations of the principle of non-intervention or the right to self-determination, but not necessarily in every case.

A more flexible and broad interpretation of the legal norms may therefore be needed to allow them to encompass these activities.

However, some of the actions described here – such as cyberattacks – have, under certain circumstances, already been recognised as violations of international law by both states[29] and the doctrine of international law.[30] Therefore, if such actions can be attributed to Russia, it could be held responsible for them.

29 Cyber Law Toolkit, 'National Position', NATO Cooperative Cyber Defence Centre of Excellence, https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

30 See Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

Armed NSAs

By Magda Long

Key takeaways

- Armed non-state actors (ANSAs) act as enforcers, disruptors, and emissaries of influence, offering deniability, operational flexibility, and local familiarity that enable the Kremlin to evade attribution, accountability, and legal responsibility.
- While their defining feature is the use of violence, this is not exclusive, as they can also contribute other valuable assets, infrastructure, and capabilities to the regime.
- Security forces, industry giants, and senior political figures have been directly or indirectly implicated in orchestrating their activities.
- Nevertheless, the clandestine and often volatile nature of these relationships complicates efforts to trace direct coordination or responsibility.

Introduction

Russia's reliance on ANSAs is a deeply embedded feature of its strategic culture – one that extends state power while retaining a veneer of deniability.[31] Although a relatively small subset of Russia's "grey zone" arsenal, their impact is strategic, lethal, and outsised.[32] From assassinations and manipulation of regional dynamics to territorial occupations and political subversion in Europe, Africa, the Middle East, and Central Asia, ANSAs act as force multipliers and strategic coercive mechanisms serving the Kremlin's objectives.

The ANSA category includes private military companies (PMCs),[33] transnational criminal networks (TCNs), paramilitary formations, militias, and terrorist groups. Contract killers and disposable agents, who are not necessarily linked to actors in the remaining sub-categories,

31 Cormac and Aldrich, 'Grey is the New Black', 477–494.

32 Giannopoulos, Smith, and Theocharidou, 'The Landscape of Hybrid Threats',10; Mark Galeotti, 'Gangster Geopolitics: The Kremlin's Use of Criminals as Assets Abroad', Russia Matters blog, Harvard Kennedy School, Belfer Center for Science and International Affairs, 17 January 2019, https://www.russiamatters.org/analysis/gangster-geopolitics-kremlins-use-criminals-assets-abroad.

33 PMCs are sometimes also referred to as private military and security companies (PMSCs), while private security companies (PSCs) are at times placed in the same category. However, the three occupy distinct roles in the privatised force spectrum. PMCs typically provide military-related services such as combat support, training, strategic planning, intelligence, and logistics support in conflict zones. Their personnel are often drawn from former military and intelligence services ranks, and their activities may include direct engagement in hostilities. In contrast, PSCs provide defensive services, including personnel protection, site security, and risk assessment. They generally operate in peacetime or low-intensity environments and avoid combat roles. PMSCs serve as an umbrella category that encompasses both PMCs and PSCs, reflecting the growing convergence of functions in the industry. While many companies blur the lines between military and security services, their legal status, degree of combat involvement, and proximity to state or corporate clients help to differentiate between them. These distinctions are critical, as Russia has made a point of attempting to differentiate between the two: PMCs are not legally permitted to register in Russia, whereas PSCs are. See 'Kremlin: No Private Military Companies Exist in Russia', TASS, 21 December 2018, https://tass.com/defense/1037365. China has ostensibly taken a similar approach. See Max Makusen, 'A Stealth Industry: The Quiet Expansion of Chinese Private Security Companies', Center for Strategic & International Studies, 12 January 2022, https://www.csis.org/analysis/stealth-industry-quiet-expansion-chinese-private-security-companies#:~:text=PMCs%20and%20PSCs:%20Both%20PMCs,Russian%20and%20partner%20combat%20operations.

also fall under this umbrella when deployed for political violence or covert subversion. **Driven by ideology, profit, or a combination of the two, ANSAs thrive in spaces where legality is ambiguous, and governance contested.** Nationalism often masks profiteering and institutional corruption, while legitimising state-sanctioned irregularity. The Kremlin mobilises ANSAs regardless of their legal standing; what matters is operational utility.[34]

PMCs and TCNs in particular have become integral to Russia's "grey zone" strategy. Since 2012, when Vladimir Putin publicly endorsed PMCs as a tool for pursuing "national interests without the direct involvement of the state",[35] ANSAs more broadly have become the Kremlin's multipurpose instrument – a Swiss army knife rather than a finely tuned scalpel – for covert strategic coercion.

Frequently, **ANSAs are interlinked, making it increasingly difficult not only to decouple their activities but also to determine the extent to which these are coordinated – directly, tacitly, or not at all – by state actors.**[36] Nevertheless, security forces,[37] industry giants, and occasionally even senior political figures have been directly or indirectly implicated in ANSAs' activities.

This chapter unpacks the seven sub-categories of ANSAs, highlighting their roles, characteristics, and value to the Kremlin (see **Figure A1**). While not all Russian ANSAs can be covered comprehensively, short vignettes will be used to illustrate how these actors support Moscow's aims while shaping the broader conflict environment.

Private military companies

As of 2021, at least 27 Russian PMCs were active and operating in 27 countries – up from four in 2015.[38] They are active throughout Africa, the Middle East, Europe, Central Asia, and Latin America. While their organisational structures, roles, and objectives vary, most maintain ties

34 Galeotti, 'Gangster Geopolitics'.

35 'Russia May Consider Establishing Private Military Companies', Sputnik International, 12 April 2012, https://sputnikglobe.com/20120412/172789099.html. In 2018, the Kremlin spokesman Dmitry Peskov insisted that Putin's endorsement of PMCs referred only to "private security and not private military activity" and that by law, no PMCs existed in Russia. See 'Kremlin: No Private Military Companies Exist in Russia'.

36 See Vladimir Rauta, 'Countering State-Sponsored Proxies: Designing a Robust Policy', Hybrid CoE Paper 23 (Hybrid CoE, February 2025), https://www.hybridcoe.fi/wp-content/uploads/2025/02/web_Hybrid_CoE_Paper-23_rgb.pdf.

37 GRU, FSB, the MoD and *Rosgvardiya*.

38 An additional 10 companies that Molfar, an OSINT company, identified appear to be inactive. See 'Catalog of Russian PMCs: 37 Private Military Companies of the Russian Federation', Molfar, March 2023, https://molfar.com/en/blog/catalog-of-russian-pmcs; Seth G. Jones et al., 'Russia's Corporate Soldiers', Center for Strategic and International Studies, July 2021, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210721_Jones_Russia%27s_Corporate_Soldiers.pdf?VersionId=7fy3TGV3HqDtRKoe8vDq2J2GGVz7N586.

to the MoD, FSB, GRU, or state-owned energy giants.[39]

PMCs occupy a central role in Russia's broader coercive diplomacy and hybrid threat strategy. It is therefore crucial to view Russian PMCs not just in terms of force multipliers in combat operations or as the Kremlin's deniable vehicles, but also in terms of their ability to:

- Expand Moscow's influence openly;
- Increase revenue streams to elites, officials, institutions, and oligarchs;
- Present Russia as an indispensable mediator and security partner in the Middle East and North Africa;
- Gain military access rights and economic concessions.[40]

PMCs remain technically illegal in Russia,[41] a status that grants the Kremlin deniability and narrative control, shielding it from legal responsibility for activities undertaken by PMCs abroad on its behalf and from accountability at home. PMC casualties are not considered military deaths, and their families receive no state benefits – ironically, the very critique

39 In 2023, Gazprom launched three PMCs – Potok, Fakel, and Plamya – promising its employees official MoD contracts but deploying them instead to Ukraine under Redut PMC. Redut PMC is also known as the Regional Laboratory of Social and Psychological Research, or specifically, GRU Unit 35555. See Yelizaveta Fokht and Il'ya Barabanov, 'Potok pod Bakhmutom. Chto izvestno o CHVK, Svyazannykh s Gazpromom', BBC News Russkaya Sluzhba, 16 May 2023, https://www.bbc.com/russian/features-65602020; Mark Krutov, Sergey Dobrynin, and RFE/RL's Idel. Realities, 'Redut,' BARS, 'Don,' 'Potok': Kakiye v Rossii Deystvuyut ChVK, Krome 'Vagnera,' i Kto za Nimi Stoit', Nastoyashcheye Vremya, 23 May 2023, https://www.currenttime.tv/a/russian-private-military-companies/32422559.html; Mark Krutov, Sergey Dobrynin, and RFE/RL's Idel. Realities, 'Who's Who Among Russia's Mercenary Companies', RFE/RL, 23 May 2023, https://www.rferl.org/a/russia-other-mercenary-companies-ukraine/32424520.html.

40 'Annual Threat Assessment of the US Intelligence Community' (Office of the Director of National Intelligence, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf; 'Chastnyee voyenno-okhrannyye organizatsii poluchat ofitsial'nyy status', Rossiyskaya Gazeta, 14 December 2015, https://rg.ru/2015/12/14/chop-anons.html.

41 Articles 208 and 359 of Russia's 1996 Criminal Code prohibit the creation, management, financing, and use of armed groups in armed conflicts – yet enforcement is selective, and deliberately so. Article 208 refers to "band, squad, militia or another group... [not] ... stipulated in a federal law", while Article 359 criminalises the "recruitment, training, financing, or any other material provision of a mercenary", and their use in an armed conflict or hostilities. See The Criminal Code of the Russian Federation, https://sherloc.unodc.org/cld/uploads/res/document/rus/1996/the_criminal_code_of_the_russian_federation_english_html/the_Criminal_Code_of_Russian_Federation_English.pdf; 'Kremlin Blocks the Bill Legalizing Russian Private Military Companies', UAWire, 28 March 2018, https://uawire.org/russia-will-not-legalize-mercenaries; Kimberly Marten, 'The GRU, Yevgeny Prigozhin, and Russia's Wagner Group', testimony before the U.S. House of Representatives Committee on Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment, 7 July 2020, https://www.congress.gov/116/meeting/house/110854/witnesses/HHRG-116-FA14-Wstate-MartenK-20200707.pdf.

Russian commentators once levelled at the West.[42] At the same time, since at least 2012, President Putin and Chief of General Staff Valery Gerasimov have publicly invoked Western PMC use as evidence of reliance on deniable force projection and imperialism – framing the Kremlin's own adoption as reactive and justified.[43]

Certain PMCs were evidently permitted to incorporate in Russia, and even those that were incorporated elsewhere became the Kremlin's useful tool.[44] **RSB Group**, founded in 2005 by former intelligence officer Oleg Krynytsyn, was incorporated both in Russia and in the British Virgin Islands for missions abroad.[45] RSB, which markets itself as a "military consulting company", resembles the American PMC model (see **Table A1**). Its personnel include "professional military personnel, as well as reserve officers" of the GRU and FSB, and it was sanctioned for training Russian forces for the war in Ukraine.[46]

Similarly, **Moran Security Group**, founded by a former KGB and later FSB officers, was registered in both Belize and Russia in 2011. Moran created the **Slavonic Corps**, Wagner Group's predecessor, which was incorporated in Hong Kong in 2013. All three companies had links to the Kremlin, the MoD, the GRU, and the FSB, and have provided services to the Russian

42 The US intelligence community estimates that the number of casualties in Ukraine has surpassed that of all of Russia's other wars "since World War II (750,000-plus dead and wounded)". See 'Annual Threat Assessment of the US Intelligence Community' (Office of the Director of National Intelligence, 2025), 22, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf; Chas Danner, 'Leaked Pentagon Documents: What We Know', New York Intelligencer, 14 May 2023, https://nymag.com/intelligencer/article/leaked-pentagon-documents-what-we-know.html; Aleksey Aleksandrov, 'Ikh chasto ispol'zuyut kak pushechnoye myaso. Chto izvestno o rabote chastnykh voyennykh kompaniy na voyne v Ukraine', Nastoyashcheye Vremya, 11 August 2022, https://www.currenttime.tv/a/chto-izvestno-o-rabote-chastnyh-voennyh-kompaniy-na-voyne-v-ukraine/31983571.html; Mikhail Andreev, 'V Gosdume prizvali uregulirovat' status CHVK Vagner v Rossii', Overclockers, 13 February 2023, https://overclockers.ru/world/show/124015/v-gosdume-prizvali-uregulirovat-status-chvk-vagner-v-rossii; Aleksandr Khramchikhin, 'ChVK: Nayemniki ili Provodniki Voli Kremlya? Pochemu v Rossii ne Khotyat Legalizovat Chastnyye Voyennyye Kompanii', Nezavisimoye Voyennoye Obozreniye, 20 April 2018, https://nvo.ng.ru/realty/2018–04–20/1_993_chvk.html.

43 See Khramchikhin, 'ChVK: Nayemniki ili Provodniki Voli Kremlya'; 'Kremlin: No Private Military Companies Exist in Russia'; Seth G. Jones, *Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare* (W. W. Norton & Company, Inc., 2021).

44 See Margarete Klein, 'Private Military Companies – A Growing Instrument in Russia's Foreign and Security Policy Toolbox', Hybrid CoE Strategic Analysis 17 (Hybrid CoE, June 2019), https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-17–2019.pdf.

45 Pavel Felgenhauer, 'Private Military Companies Forming Vanguard of Russian Foreign Options', The Jamestown Foundation, 16 March 2017, https://jamestown.org/program/private-military-companies-forming-vanguard-russian-foreign-operations/; 'RSB Group', Open Sanctions, 15 April 2025, https://www.opensanctions.org/entities/NK-XvbFxD8YzfK5JHq68o2n4x/; 'Oleg Krinytsin', Executive.ru, https://www.e-xecutive.ru/users/92919-oleg-krinitsyn; 'Oleg Anatolyevich Krinitsyn', Open Sanctions, 15 April 2025, https://www.opensanctions.org/entities/NK-BndfTMx2fZqsz58Qv64×9x/.

46 Open Sanctions, 'RSB Group'.

state in Africa, the Middle East, and Ukraine.[47] While this Moran Security Group reportedly dissolved in 2017,[48] a company by the same name, which has existed since 1999 according to its website, appears to be active and is led by Igor Nikov, a former Russian Navy officer.[49]

PMC Patriot, backed by Sergei Shoigu, has operated in Burundi, the Central African Republic (CAR), Syria, Yemen, Sudan, Gabon, and Ukraine since it was founded in 2018.[50] **PMC Paladin**, by contrast, appears to deviate from the Kremlin-aligned messaging. Established in 2022 by Georgy Zakrevsky and based in Moscow, Paladin brands itself explicitly as a PMC[51] and claims deployments in Lebanon, the Democratic Republic of the Congo, and Ecuador, although it has reportedly also operated in Ukraine and possibly in Syria at some point.[52] Most strikingly, in August 2024, Zakrevsky made headlines with a viral video publicly denouncing Putin, holding him responsible for failures in Ukraine and for Russian social and economic decline, and calling for regime change.[53]

The Wagner Group, which emerged during Russia's annexation of Crimea, became the archetypal Kremlin-aligned PMC, with a hydra-like, clandestine network of shell companies numbering in the hundreds.[54] Wagner may have been the Kremlin's muscle, it was riding on the back of mafia logistics. Its criminal

47 Krutov, Dobrynin, and RFE/RL's Idel. Realities, 'Who's Who Among Russia's Mercenary Companies'; Ase Gilje Ostensen and Tor Bukkvoll, 'Private Military Companies – Russian Great Power Politics on the Cheap?', *Small Wars & Insurgencies*, Volume 33, Issues 1–2 (2022): 130–151; Ilya Barabanov and Denis Korotkov, *Nash Biznes Smyert: Polnaya Istoriya ChVK Wagner i yye Osnovatelya Yevgenia Prigozhina* (SIA Meduza Project 2024), 88–89.

48 'Tovarystvo z obmezhenoyu vidpovidal'nistyu "Moran Sekyuriti Hrup"', Open Sanctions, 29 October 2025, https://www.opensanctions.org/entities/NK-eQStdcgF763BDUkRNezydV/.

49 Moran Security Group website, https://moran-group.ru/en/about/index.

50 Shoigu is the Secretary of the Russian Federation Security Council and formerly the Minister of Defence. See 'PMC Patriot', Open Sanctions, 9 April 2025, https://www.opensanctions.org/entities/NK-oN4V9PcudbqqHzBgaZWCfc/; Jones et al., 'Russia's Corporate Soldiers'.

51 Registration documents apparently show that Paladin was registered only in 2022 as an organisation engaged in "professional, scientific and technical activities". See 'Paladin', https://paladinkrite.com/#rec559092024; Konstantin Dovgan, 'Agent FSB i novyy Prigozhin? Kto takoy Georgiy Zakrevskiy i real'ny li yego ugrozy Putinu', 24 Kanal, 17 August 2024, https://24tv.ua/ru/georgij-zakrevskij-biografija-vladelca-chvk-paladin-javljaetsja_n2619096; The company's website is also shared by the Military Union Paladin (Voinskiy soyuz Paladin) on a Telegram channel. Voinskiy soyuz Paladin, @VSPaladin2024, TGStat, https://tgstat.ru/channel/@VSPaladin2024.

52 Dovgan, 'Agent FSB i novyy Prigozhin?'.

53 Dovgan, 'Agent FSB i novyy Prigozhin?'; Alexander J. Motyl, 'Another Russian Mercenary Leader Has Turned Against Putin', The Hill, 22 August, 2024, https://thehill.com/opinion/international/4839613-another-russian-mercenary-leader-has-turned-against-putin/.

54 Barabanov and Korotkov, *Nash Biznes – Smyert*, 88–89; Jack Margolin, *The Wagner Group: Inside Russia's Mercenary Army* (London: Reaktion Books Ltd., 2024), 169; Olivia Allison, Nick Connon, Antonio Giustozzi, and James Pascall, 'Wagner's Business Model in Syria and Africa: Profit and Patronage', RUSI Occasional Paper (RUSI, February 2025), https://static.rusi.org/wagners-business-model-in-syria-and-africa_0.pdf.

CASE STUDY 1: Violence by Russia's PMCs and their affiliates

Wagner fighters have been accused of violating international law and killing civilians in virtually all the countries where they have operated militarily since 2014.

The US Treasury Department designated Wagner a significant transnational criminal organisation, citing serious criminal activities "including mass executions, rape, child abductions, and physical abuse in the CAR and Mali".

In July 2023, the UK government sanctioned Sewa Security Services (SSS), a CAR-based security company, for undermining and threatening the peace, stability, and security of the CAR, and for providing cover for Wagner operations there.

SSS provides protection for senior CAR government officials and has also been implicated in violent attacks that have taken place in the CAR since the December 2020 presidential election.

identity not only attracted criminals but also normalised their behaviour.[55] After its 2023 mutiny, Wagner's remnants were rebranded as the **Expeditionary Corps**, including **Africa Corps**, led by **Andrei Averyanov**, head of the infamous GRU Unit 29155 and deputy head of the GRU, and the **Volunteer Corps**. Some Wagner fighters joined the ***Rosgvardiya* Volunteer Corps** for deployments abroad, despite *Rosgvardiya's* domestic mandate.[56]

What is particularly concerning is that some of these groups have exhibited extreme violence and brutality against civilians – for example, Wagner and its affiliated company Sewa Security Services (see **Case Study 1**) – as well as the sheer number of clandestine companies and affiliations linked to Russian PMCs.[57] They also often overlap with extreme-right, white supremacist paramilitary formations such as **DShRG Rusich** and the **Russian Imperial Movement** (RIM), including its military wing, **the Russian Imperial Legion**, and are characterised by general criminality.

Transnational criminal networks

The Kremlin weaponises TCNs as deniable auxiliaries of state power, co-opting them into intelligence operations, sabotage, and influence campaigns. These networks – comprising arms and drug traffickers, smugglers, money launderers, forgers, cybercriminals, and enforcers – are far from mere rogue elements.

The FSB pioneered this tactic in the 1980s, cultivating informants and assets within domestic gangs and extremist circles. Over time, these links evolved into a broader external toolkit for projecting covert power.[58] **Since 2014, and even more so after 2022, Russia has**

55 'Treasury Sanctions Russian Proxy Wagner Group', Department of the Treasury, https://home.treasury.gov/news/press-releases/jy1581; Anna Arutunyan and Mark Galeotti, *Downfall: Prigozhin, Putin and the New Fight for the Future of Russia*, iPad edition (Ebury Press, 2024), 113; Kimberly Marten, 'Where's Wagner Now? One Year After the Mutiny', PONARS Eurasia Policy Memo No. 903 (June, 2024), https://www.ponarseurasia.org/wheres-wagner-now-one-year-after-the-mutiny/.

56 Seth Jones, '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; Marten, 'Where's Wagner Now?'.

57 Foreign Affairs Committee, 'Guns for Gold: The Wagner Network Exposed', UK Parliament, 26 July 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/167/report.html#footnote-229-backlink; US Department of the Treasury, 'Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization', 26 January 2023, https://home.treasury.gov/news/press-releases/jy1220; Foreign, Commonwealth & Development Office, 'UK Sanctions Wagner Group Leaders and Front Companies Responsible for Violence and Instability Across Africa', 20 July 2023, https://www.gov.uk/government/news/uk-sanctions-wagner-group-leaders-and-front-companies-responsible-for-violence-and-instability-across-africa; 'Sewa Security Services', Open Sanctions, 2 June 2025, https://www.opensanctions.org/entities/NK-g4YnaxJbdXa7Cd2mpzrg84/.

58 Mark Galeotti, 'Gangsters at War: Russia's Use of Organized Crime as an Instrument of Statecraft', Global Initiative Against Transnational Organized Crime Research Report (GI-TOC, November, 2024), 18, https://globalinitiative.net/wp-content/uploads/2024/10/Mark-Galeotti-Gangsters-at-war-Russias-use-of-organized-crime-as-an-instrument-of-statecraft-GI-TOC-November-2024.pdf.

CASE STUDY 2: The interconnected nature of ANSAs

Use of ANSAs against Montenegro	Russia's attempted coup in Montenegro in 2016 involved a constellation of actors, including GRU Unit 29155, criminal actors, PMCs, paramilitary formations, and militia elements. GRU officers Eduard Shishmakov and Vladimir Popov – sentenced in absentia by the Supreme Court of Montenegro to 15 and 12 years in prison respectively – coordinated with Serbian nationalist and Donbas war veteran Aleksandar Sindjelić to execute a violent takeover of the Montenegrin parliament on election day. Their objective was to prevent Montenegro's accession to NATO and install a pro-Russian government under the guise of a nationalist revolution. The GRU channelled hundreds of thousands of euros through criminal intermediaries to finance weapons procurement, fake police uniforms, encrypted communication devices, and travel logistics. The network extended to Chechen criminal intermediaries associated with Ramzan Kadyrov, who were tasked with persuading the Muslims to support the coup's outcome. Other actors included figures like GRU officer Viktor Boyarkin – believed to be linked to sanctioned oligarch Oleg Deripaska, Serbian organised crime figures such as Sindjelic, and former FSB officer Daniil Martynov. Their collaboration highlights the convergence of state intelligence, oligarchic influence, and criminal muscle in Russian hybrid threat operations.

increasingly outsourced the "dark aspect" of statecraft to criminal actors with transnational reach and built-in deniability. As RUSI Senior Associate Fellow Mark Galeotti notes, the scale and institutionalisation of this practice under Putin far exceeds that of the Soviet era.[59] As shown in **Case Study 2**, TCNs are closely linked to other ANSAs and can participate in intricately coordinated and high-stakes hybrid threat operations, such as the 2016 Montenegro coup.[60]

Similar dynamics unfolded in Crimea and Donbas, where the infamous "little green men" and local criminals helped seize territory before being integrated into separatist structures. This trend accelerated following the 2022 invasion of Ukraine, with reports of Chechen TCNs liaising with Ukrainian criminals in an effort to co-opt them – echoing the Kremlin's 2014 invasion playbook.[61]

TCNs have long been consolidated under the control of oligarchs linked to President Putin or Russian intelligence and have been allowed to profit freely as long as they supported the Kremlin's priorities.[62] Some of this support includes weapons trafficking, smuggling, laundering of sanctioned assets, and the procurement of dual-use technologies. Europol and European intelligence agencies have observed a surge in sabotage, smuggling, and cybercrime connected to Russia-based networks since the invasion of Ukraine.[63] **TCNs also help generate *chernaya kassa* ("black cashbox")**

59 Galeotti, 'Gangsters at War'; Galeotti, 'Gangster Geopolitics'.

60 See Christo Grozev, 'The Kremlin's Balkan Gambit: Part I', Bellingcat and the Insider, 4 March 2017, https://www.bellingcat.com/news/uk-and-europe/2017/03/04/kremlins-balkan-gambit-part/; 'Kome je Sve OSA Zabranila Ulazak u BiH: Od Putinovog Oligarha Malofeeva, Preko Vođe Noćnih Vukova Aleksandra Zaldostanova do Karadžićevog Advokata Petronijevića', Istraga.ba, 25 March 2022, https://istraga.ba/kome-je-sve-osa-zabranila-ulazak-u-bih-od-putinovog-oligarha-malofeeva-preko-vode-nocnih-vukova-aleksandra-zaldostanova-do-karadzicevog-advokata-petronijevica/.

61 Galeotti, 'Gangster Geopolitics'; Watling, Danylyuk, and Reynolds, 'The Threat from Russia's Unconventional Warfare Beyond Ukraine', 12; See also Magda Long, 'Shadows of Power Beneath the Threshold: Where Covert Action, Organized Crime and Irregular Warfare Converge', *Intelligence & National Security*, Volume 40, Issue 2 (October, 2024): 1–27.

62 Michael Prothero, 'Russian Spies Have Gone Full Mafia Mode Because of Ukraine', VICE, 27 October 2022, https://www.vice.com/en/article/russia-traffickers-spies/; Watling, Danylyuk, and Reynolds, 'The Threat from Russia's Unconventional Warfare Beyond Ukraine', 12.

63 'European Union Serious and Organised Crime Threat Assessment: The Changing DNA of Serious and Organised Crime' (Publications Office of the European Union, 2025), https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime; Mitchell Prothero, 'Russian Spies Have Gone Full Mafia Mode Because of Ukraine'; Galeotti, 'Gangsters at War'.

TABLE 1. Spectrum of paramilitary formations

Loosely connected	Institutionally connected	Covertly supported	Officially sanctioned
Formations that the state tolerates but does not directly organise.	Formations comprising off-duty police or army officers, but supported by individuals (e.g., businessmen or politicians) rather than state institutions directly.	Formations that may receive covert support while presenting themselves as grassroots or independent.	Auxiliaries that are formally approved and sometimes integrated into the state's coercive apparatus.

for the Kremlin, used to bankroll covert operations, pay bribes and agents, run influence campaigns, and provide the FSB and GRU with the infrastructure needed to establish shell companies, safe houses, and smuggling routes.[64]

The increasing trend of layered outsourcing among ANSAs is particularly concerning. Russia-based TCNs subcontract activities to local criminal groups across Europe, and this symbiosis gives the Kremlin access to resources typically reserved for TCNs, allowing Moscow to harvest criminal intelligence, launder resources, and extend strategic goodwill to them when useful.[65] These actors, however, are often unreliable, self-interested, and unpredictable, and their cooperation exposes the state to reciprocal exploitation.[66]

Paramilitary formations

Although the term *paramilitary* is often loosely applied to PMCs, the two differ in legal status, structure, and purpose. PMCs are commercial enterprises driven by profit, offering services that range from combat support to logistics within a transactional framework. **Paramilitary formations are not formal state organs but may operate in alignment with state objectives or ideology.** They may receive state support, operate alongside formal military structures, or even be absorbed into official structures while maintaining a degree of autonomy. **Table 1** illustrates the spectrum of paramilitary formations; in the Russian context, however, these distinctions are even more convoluted.[67]

Groups such as **Rusich** and **RIM** embody the fusion of paramilitarism and other armed non-state activity. These extreme-right, white supremacist militant organisations have long histories of aligning with Russian interests.[68] Both Rusich and RIM fought alongside separatists in Ukraine in 2014 and re-emerged in support of Russia's 2022 invasion.[69] In 2015, Rusich fighters were filmed mutilating Ukrainian soldiers, yet despite (or perhaps because) of their notoriety the FSB Border Service reportedly

64 Galeotti, 'Gangster Geopolitics'; Galeotti, 'Gangsters at War'; Magnus Normark, 'How States Use Non-State Actors'; Watling, Danylyuk, and Reynolds, 'The Threat from Russia's Unconventional Warfare Beyond Ukraine', 12; Jones et al., 'Russia's Corporate Soldiers'.

65 Galeotti, 'Gangsters at War'.

66 Galeotti, 'Gangster Geopolitics'; Long, 'Shadows of Power Beneath the Threshold'.

67 See Uğur Ümit Üngör, *Paramilitarism: Mass Violence in the Shadow of the State* (Oxford University Press, 2020), 7; Andrew Thomson and Dale Pankhurst, 'From Control to Conflict: A Spectrum and Framework for Understanding Government-Militia Relationships', *Studies in Conflict & Terrorism*, Volume 48, Issue 6 (2025), https://www.tandfonline.com/doi/full/10.1080/1057610X.2022.2116972.

68 Wagner's co-founder and former GRU member, the recently deceased Dmitry Utkin, was reportedly a neo-Nazi himself. See Denis Korotkov, 'Khayl' Petrovich': Istoriya Dmitriya Utkina – Cheloveka, Kotoryy Podaril Gruppe Vagnera Nazvaniye', Dosye, 10 April 2023, https://dossier.center/utkin/.

69 Mark Townsend, 'Russian Mercenaries in Ukraine Linked to Far-Right Extremists', The Guardian, 20 March 2022, https://www.theguardian.com/world/2022/mar/20/russian-mercenaries-in-ukraine-linked-to-far-right-extremists; 'Russian Imperial Movement', Mapping Militant Organizations, https://mappingmilitants.org/profiles/russian-imperial-movement#strategy; Candace Rondeaux, Ben Dalton, and Jonathan Deer, 'Wagner Group Contingent Rusich on the Move Again', New America, 26 January 2022, https://www.newamerica.org/future-frontlines/blogs/wagner-group-contingent-rusich-on-the-move-again/.

engaged Rusich for intelligence operations and to reinforce the border with Finland.[70] RIM was designated a terrorist organisation by the US in 2020 for training white supremacists and neo-Nazis in Europe.[71] RIM's Partisan training programme provides recruits with tactical training and ideological indoctrination, alongside lectures on NATO and how to interrogate a captured adversary in English, suggesting ambitions that extend beyond Ukraine.[72] This apparent contradiction – invoking *denazification* in Ukraine while deploying neo-Nazi militants – underscores Moscow's instrumentalist approach to adversarial symbioses.[73]

Paramilitary formations such as Rusich, RIM, and their ideological successors remain strategically useful to the Kremlin, at least for now. They provide manpower for sabotage, propaganda, territorial disruption, and psychological operations.[74] Operating along NATO's eastern flank, they seek to undermine regional stability, destabilise neighbours, and erode democratic resilience.[75] **The ideological militancy of these formations makes them**

70 'Task Force Rusich', Open Sanctions, 16 April 2025, https://www.opensanctions.org/entities/NK-SGoKLj97jDeyJGnSyRhJJN/; 'DShRG Rusich: A Neo-Nazi Unit in the Service of the Russian Armed Forces', Molfar, 12 January 2023, https://molfar.com/en/blog/dshrg-rusich; Thomas Nilsen and Olesia Krivtsova, 'Neo-Nazi Mercenaries to Help FSB Guard Border with Finland', The Barents Observer, 10 September 2024, https://www.thebarentsobserver.com/borders/neonazi-mercenaries-to-help-fsb-guard-border-with-finland/101159.

71 'United States Designates Russian Imperial Movement and Leaders as Global Terrorists', US Department of State, 7 April 2020, https://2017–2021.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists/; 'Inside the Russian Imperial Movement: Practical Implications of US Sanctions', Special Report (The Soufan Center, April 2020), https://thesoufancenter.org/wp-content/uploads/2020/06/TSC-Report-Inside-the-Russian-Imperial-Movement-Practical-Implications-of-US-Sanctions.pdf; Lucas Webber and Alec Bertina, 'The Russian Imperial Movement in the Ukraine Wars: 2014–2023', CTC Sentinel, Volume 16, Issue 11 (August, 2023) 23–31, https://ctc.westpoint.edu/wp-content/uploads/2023/08/CTC-SENTINEL-082023.pdf.

72 'Inside the Russian Imperial Movement', 20.

73 Townsend, 'Russian Mercenaries in Ukraine Linked to Far-Right Extremists'.

74 Another example is E.N.O.T. Corp, a now-defunct group straddling the line between a nationalist paramilitary formation and a PMC. Founded by far-right agitator Igor Mangushev, E.N.O.T. operated in Tajikistan and Nagorno-Karabakh, and ran patriotic, militaristic youth camps in Serbia, Montenegro, and Belarus. Its co-founder, Roman Telenkevich, was sentenced in 2022 to 13 years in prison for extortion, and several other members, including former federal security or intelligence officers, were investigated for robbery and extortion. See 'Russian Officer Who Brandished Alleged Ukrainian Skull Dies of Gunshot Wound', Radio Free Europe/Radio Liberty, 8 February 2023, https://www.rferl.org/a/russia-officer-skull-dead-gunshot-wound-mangushev/32261774.html; Krutov, Dobrynin, and RFE/RL's Idel. Realities, 'Who's Who Among Russia's Mercenary Companies'.

75 For instance, Rusich's official Telegram channel reportedly urged its members in the Baltic NATO countries to gather data on the location of border checkpoints, surveillance systems, telecommunication towers, military units, and on soldiers and their relatives. See 'Russian Neo-Nazi Group Rusich "Collecting Intelligence About Military Objects in Baltic"', The New Voice of Ukraine, 12 December 2022, https://english.nv.ua/nation/russian-neo-nazi-group-rusich-collecting-intelligence-about-military-objects-in-baltic-50290279.html; Mark Townsend, 'Neo-Nazi Russian Militia Appeals for Intelligence on NATO Member States', The Guardian,

less controllable than regular forces or even PMCs. However, their violent activities, symbolic provocations, and embedded presence in "grey zone" operations enable Moscow to exert pressure while disavowing responsibility.

Militias

Militias provide a ready-made infrastructure for territorial control, coercion, counterinsurgency, and intimidation without the professionalism or profit motives of PMCs, or the battlefield specialisation associated with paramilitary formations.

Militias serve as shock troops, enforcers, and cultural emissaries for shaping local power dynamics under the veneer of deniability. They originate from volunteer or ideological communities, unlike paramilitary formations that typically operate *on behalf of*, alongside, or beyond the state. While militias may align with state interests, they remain semi-autonomous coercive entities, lacking formal incorporation into state command structures.[76]

A central example is the **Kadyrovtsy** – the personal militia of Chechen leader Ramzan Kadyrov – known for cruelty and abuse, while invoking fear and psychological pressure. Formally under the *Rosgvardiya*, Putin's own Praetorian guard, the Kadyrovtsy act autonomously and remain loyal to Kadyrov. In return for loyalty and repression in Chechnya, Kadyrov enjoys patronage and influence.[77]

The Kadyrovtsy have been deployed to Georgia, Syria, Libya, and Ukraine. Their units include the Akhmat Grozny OMON, responsible for riot control and policing, while the elite wing, Akhmat SOBR,[78] functions as a regional militia.[79]

In Ukraine, Akhmat units were deployed as volunteers under MoD contracts, demonstrating the loyalty that Wagner later refused. They assumed law enforcement duties around the Zaporizhzhia nuclear power plant and replaced

https://www.theguardian.com/world/2022/dec/11/neo-nazi-russian-militia-appeals-for-intelligence-on-nato-member-states; Kacper Rekawek, Thomas Renard, and Bàrbara Molas, (eds.), *Russia and the Far-Right: Insights from Ten European Countries* (ICCT Press, 2024), https://icct.nl/sites/default/files/2024-04/Russia%20and%20the%20Far-Right%20Insights%20from%20Ten%20European%20Countries%20-%20A4%20e-book_0.pdf.

76 Üngör, *Paramilitarism*, 8.

77 Laura Linderman and Anna Harvey, 'Kadyrov's Chechnya: The State Within Putin's State', The Central Asia-Caucasus Analyst, 17 April 2025, https://www.cacianalyst.org/resources/Kadyrovs_Chechnya_The_State_Within_Putins_State_final.pdf, 2, 6; Sam Cranny-Evans, 'The Chechens: Putin's Loyal Foot Soldiers', RUSI Commentary, 4 November 2022, https://www.rusi.org/explore-our-research/publications/commentary/chechens-putins-loyal-foot-soldiers; Justin Ling, 'Russia Tries to Terrorize Ukraine With Images of Chechen Soldiers', Foreign Policy, 26 February 2022, https://foreignpolicy.com/2022/02/26/russia-chechen-propaganda-ukraine/; Munira Mustaffa, 'The Kadyrovtsy: Putin's Force Multiplier or Propaganda Tool?' New Lines Institute, 4 March 2022, https://newlinesinstitute.org/state-resilience-fragility/the-kadyrovtsy-putins-force-multiplier-or-propaganda-tool/#:~:text=Their%20zeal%20to%20exact%20personal,of%20the%20New%20Lines%20Institute.

78 Formerly known as Terek.

79 Linderman and Harvey, 'Kadyrov's Chechnya', 2, 6; Marten, 'Where's Wagner Now?'; Cranny-Evans, 'The Chechens'.

Wagner units in Bakhmut. Some Wagner fighters were even absorbed into Akhmat after the 2023 mutiny, despite prior rivalries between Yevgeniy Prigozhin and Kadyrov.[80]

Ideological militias such as the Cossacks and the Night Wolves represent a long-standing Russian tradition of community-based militarisation. Over 17,500 registered **Cossack** troops reportedly fought in Ukraine, forming volunteer battalions in occupied territories in Crimea and possibly in Donetsk, Luhansk, Kherson, and Zaporizhzhia.[81] While the Cossacks' historical role as social enforcers for the regime[82] lends cultural legitimacy, their current value lies in being pre-organised, armed, and deniable auxiliaries motivated by patriotism and regionalism.

The **Night Wolves**, a nationalist biker gang, act as ideological enforcers and nationalist provocateurs. Although not conventionally armed, their Kremlin and ROC ties, combined with theatrical symbolism, give them political and mobilising influence. They have received public endorsements, state funding, and honours from Kadyrov, Republika Srpska President Milorad Dodik, and Transnistrian President Vadim Krasnoselsky.[83] Their influence is particularly evident in the Western Balkans, where they have cultivated ties with paramilitary and ultranationalist groups such as **Srpska Čast**[84] and **Zavetnici**, exploiting nationalism, ethnic divisions, and anti-Western sentiment.[85]

In 2014, the Night Wolves' Sevastopol chapter actively aided the annexation of Crimea, gathering intelligence, disseminating propaganda, organising protests, securing infrastructure, and coordinating with Russian special forces. They helped establish checkpoints and intimidate officials, blending sharp power, psychological operations, and physical coercion.[86] Although Moscow leverages militias for their utility, it also asserts control

80 Marten, 'Where's Wagner Now?'; Jones et al., 'Russia's Corporate Soldiers', Chapter 3; Marlene Laruelle and Richard Arnold, 'Russia's Paramilitarization and Its Consequences', PONARS Eurasia Policy Memo No. 839 (April, 2023), https://bunny-wp-pullzone-a7uhvox9dj.b-cdn.net/wp-content/uploads/2023/04/Pepm839_Arnold-Laruelle_April2023–2.pdf.

81 Ostensen and Bukkvoll, 'Russian Use of Private Military and Security Companies'; Kira Harris, 'A Hybrid Threat: The Night Wolves Motorcycle Club', *Studies in Conflict & Terrorism*, Volume 46, Issue 9 (2023): 1784–1816. Laruelle and Arnold, 'Russia's Paramilitarization and its Consequences;' Watling, Danylyuk, and Reynolds, 'The Threat from Russia's Unconventional Warfare Beyond Ukraine'.

82 Richard Arnold, 'The Expanding Russian Cossack Movement: A Social Base for Putinism', PONARS Eurasia Policy Memo No. 774 (May, 2022), https://www.ponarseurasia.org/the-expanding-russian-cossack-movement-a-social-base-for-putinism/.

83 Harris, 'A Hybrid Threat', 1794; Normark, 'How States Use Non-State Actors'; 'Kome je Sve OSA Zabranila Ulazak u BiH: Od Putinovog Oligarha Malofeeva, Preko Vođe Noćnih Vukova Aleksandra Zaldostanova do Karadžićevog Advokata Petronijevića', Istraga.ba, 25 March, 2022, https://istraga.ba/kome-je-sve-osa-zabranila-ulazak-u-bih-od-putinovog-oligarha-malofeeva-preko-vode-nocnih-vukova-aleksandra-zaldostanova-do-karadzicevog-advokata-petronijevica/.

84 Serbian Honour.

85 Harris, 'A Hybrid Threat', 1794.

86 Matthew A. Lauder, 'Wolves of the Russian Spring: An Examination of the Night Wolves as a Proxy for the Russian Government', *Canadian Military Journal*, Volume 18, Issue 3 (2018): 5–16; Jack Losh, 'Putin's Angels: The Bikers Battling for Russia in Ukraine', The Guardian, 29 January 2016, https://www.theguardian.com/world/2016/jan/29/russian-biker-gang-in-ukraine-night-wolves-putin.

when they operate independently. Wagner was previously tasked with restraining unruly Cossack formations and neutralising separatist militias that strayed from Moscow's objectives.[87]

Terrorist groups

Russia's engagement with terrorist organisations reflects a flexible, instrumentalist approach shaped by Cold War precedent. During the Soviet era, the KGB provided training and support to a range of anti-Western violent actors spanning a wide ideological spectrum, from Hamas to the Red Army Faction.[88]

While Moscow publicly presents itself as a bulwark against terrorism, its actions suggest otherwise. **Russia does not openly sponsor terrorist groups in the conventional sense, but rather co-opts, coordinates with, or exploits them to advance its geostrategic objectives.**[89]

In the Middle East, Russia has aligned operationally with Iran-backed actors, including Hezbollah and the Houthis. Russian military forces, including PMCs, fought alongside Hezbollah in Syria, and Russian intelligence collaborated with the group to help the Assad regime evade sanctions.[90] More recently, GRU officers, operating under the guise of humanitarian aid, have provided technical assistance and intelligence for Houthi attacks on commercial shipping in the Red Sea.[91] Disturbingly, the Houthis have also been implicated in human trafficking schemes to recruit Yemeni fighters for the war in Ukraine, according to the US Treasury.[92]

87 Sergey Sukhankin, ''Continuing War by Other Means': The Case of Wagner, Russia's Premier Private Military Company in the Middle East', The Jamestown Foundation, 13 July 2018, https://jamestown.org/program/continuing-war-by-other-means-the-case-of-wagner-russias-premier-private-military-company-in-the-middle-east/#_edn44.

88 Catherine Belton, 'Did Vladimir Putin Support Anti-Western Terrorists as a Young KGB Officer?' POLITICO, 20 June 2020, https://www.politico.eu/article/did-vladimir-putin-support-anti-western-terrorists-as-a-young-kgb-officer/.

89 See Jokinen and Normark, 'Hybrid Threats from Non-State Actors'; Giannopoulos, Smith, and Theocharidou, *The Landscape of Hybrid Threats*; Anna Borshchevskaya, 'Russia's Relationship with Hamas and Putin's Global Calculations', The Washington Institute for Near East Policy, 6 November 2023, https://www.washingtoninstitute.org/policy-analysis/russias-relationship-hamas-and-putins-global-calculations; Kimberly Marten, 'Upsetting the Balance: Why Russia Chose Hamas over Israel', *The Washington Quarterly* 47, Issue 3 (2024): 79–102.

90 Aurora Ortega and Matthew Levitt, 'Hizbullah and Russia's Nascent Alliance', RUSI Commentary, 23 May 2023, https://www.rusi.org/explore-our-research/publications/commentary/hizbullah-and-russias-nascent-alliance; 'Treasury Targets Oil Smuggling Network Generating Hundreds of Millions of Dollars for Qods Force and Hizballah', US Department of the Treasury, 25 May 2022, https://home.treasury.gov/news/press-releases/jy0799.

91 'Treasury Targets Houthi Leaders Involved in Smuggling and Procuring Weapons', US Department of the Treasury, 5 March 2025, https://home.treasury.gov/news/press-releases/sb0041; Fatima Abo Alasrar, 'The United States' Houthi Terrorist Designation Unmasks Russia's Yemen Strategy', Atlantic Council, 14 March 2025, https://www.atlanticcouncil.org/blogs/menasource/houthi-terrorist-designation-russias-yemen-strategy/; Elisabeth Braw, 'Russia is Running an Undeclared War on Western Shipping', Foreign Policy, 7 November 2024, https://foreignpolicy.com/2024/11/07/russia-houthis-targeting-data-war-western-shipping-gaza/.

92 'Treasury Targets Houthi Leaders Involved in Smuggling and Procuring Weapons'.

The Kremlin's ties to terrorist groups also intersect with organised crime. Arms trafficker **Viktor Bout** has reportedly resumed operations since his release from US custody, facilitating weapons transfers to the Houthis.[93] This overlap between terrorism and organised crime is no coincidence; it is a cornerstone of Russia's shadow warfare strategy, exploiting illicit economies to sustain influence, destabilise adversaries, and maintain covert influence abroad.[94]

Moscow has also empowered and exploited violent far-right extremist groups such as the aforementioned Rusich and RIM. RIM, in particular, serves as a conduit for connecting Russian-aligned militants with like-minded Western groups. Participants in its Partizan training programme have included members of Germany's **National Democratic Party** and **The Third Path**, as well as Sweden's **Nordic Resistance Movement**, whose members carried out bomb attacks in 2017.[95]

Contract killers

Contract killers are probably among the most professionally trained and valued assets on Russia's roster of deniable actors. According to US intelligence, "the first clear case in the Putin era of Moscow directing assassination abroad occurred in 2004 in Qatar".[96] Typically linked to state agencies such as the FSB or GRU, these individuals are selected for their reliability, operational skills, and capacity for cross-border violence.[97] Their missions are likely to be tightly coordinated, often including high-value targets with potential diplomatic fallout.

In February 2024, Maksim Kuzminov – a Russian pilot who defected to Ukraine in 2023 – was assassinated in Spain in a killing that bore the signature of professional contractors. Russian authorities had made no secret of their desire to eliminate Kuzminov, and surveillance footage captured two masked men who attacked and killed him. The killers escaped, but the Spanish police noted that the operation

93 'Putin's 'Merchant of Death' Viktor Bout Returns to Arms Trading Business', The Moscow Times, 7 October 2024, https://www.themoscowtimes.com/2024/10/07/putins-merchant-of-death-viktor-bout-returns-to-arms-trading-business-wsj-a86591; Matt Potter, 'The Dark Truth About Viktor Bout', The Time, 9 December 2022, https://time.com/6240082/truth-about-viktor-bout/.

94 Magda Long, 'When State Go Mob: The Criminalization of Modern Statecraft', The Cipher Brief, 6 August 2025, https://www.thecipherbrief.com/gray-zone-criminal.

95 See 'Russian Imperial Movement (RIM)', Counter Extremism Project, https://www.counterextremism.com/threat/russian-imperial-movement-rim; Daveed Gartenstein-Ross, Samuel Hodgson, and Colin P. Clarke, 'The Russian Imperial Movement (RIM) and Its Links to the Transnational White Supremacist Extremist Movement', The International Centre for Counter-Terrorism, 24 April 2020, https://icct.nl/publication/russian-imperial-movement-rim-and-its-links-transnational-white-supremacist-extremist.

96 'Kremlin-Ordered Assassinations Abroad Will Probably Persist', Office of the Director of National Intelligence, 11 July 2016, https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rZczGbJ3×9ok/v0; Jason Leopold, 'Putin's Assassination Targets Revealed in Declassified Memo', Bloomberg, 22 November 2024, https://www.bloomberg.com/news/newsletters/2024–11–22/putin-s-assassination-targets-revealed-in-declassified-memo.

97 Galeotti, 'Gangster Geopolitics'; Annual Threat Assessment of the US Intelligence Community (Office of the Director of National Intelligence, 2021), https://www.intelligence.senate.gov/sites/default/files/documents/2021–04–09%20Final%20ATA%202021%20%20Unclassified%20Report%20-%20rev%202.pdf, 9.

pointed "to organised crime, to a criminal organisation, to professionals".[98]

Such incidents follow a long-standing pattern. In 2019, Zelimkhan Khangoshvili, a Georgian-Chechen exile and former insurgent commander, was assassinated in Berlin by Vadim Sokolov – later identified by German prosecutors as **Vadim Krasikov**, a Russian contract killer with ties to the FSB.[99] Although sentenced in Germany, Krasikov was reportedly released in an August 2024 prisoner exchange, which underlines how highly the Kremlin values such assets.[100] It is evident that this category of ANSAs is neither opportunistic nor expendable. They are instruments of highly calibrated state violence that the Kremlin reserves for cases where precision, deniability, and message-sending are paramount.

Disposable agents

Disposable agents, by contrast, are expendable actors recruited for availability rather than expertise. These actors, ranging from criminal enforcers and intelligence-linked assets to freelance saboteurs, are used for espionage, assassinations, sabotage, coercion, and other forms of targeted violence. Typically sourced through criminal intermediaries or a gig-economy recruitment approach powered by information communications technology, particularly digital platforms and apps, disposable agents are employed in operations where scale, cost, and deniability matter more than finesse or experience.[101]

The strategic utility of these actors lies in their expendability and general anonymity. Operating across borders, they enable the Kremlin to obfuscate attribution, often mimicking local criminal activity or conducting spectacularly public operations intended to send a message. Since the mass expulsion of Russian intelligence officers from Europe after 2022, reliance on these loosely affiliated, minimally vetted actors has grown markedly, demonstrating a shift from tradecraft to volume.[102]

GRU Unit 29155, in particular, has been linked to assassinations and sabotage carried out by a mix of trained assets, willing criminals, and useful idiots, often outsourced to local hires solicited via online platforms such as the Telegram messaging app. Between 2023 and 2024, the number of such attacks in Europe nearly tripled, after having already quadrupled between 2022 and 2023.[103]

98 Michael Schwirtz and Jose Bautista, 'A Russian Defector's Killing Raises Specter of Hit Squads', The New York Times, 31 March, 2024, https://www.nytimes.com/2024/03/31/world/europe/russian-defector-murder-spain.html.

99 Galeotti, 'Gangster Geopolitics', 34; Annual Threat Assessment of the US Intelligence Community, 9.

100 Matthew Kupfer, 'Who Did the West Release in Thursday's Prisoner Exchange', Voice of America, 2 August 2024, https://www.voanews.com/a/who-did-the-west-release-in-thursday-s-prisoner-exchange-/7728139.html.

101 Daniela Richterova, Elena Grossfeld, Magda Long, and Patrick Bury, 'Russian Sabotage in the Gig Economy Era', *The RUSI Journal*, Volume 169, Issue 5 (2024): 1–12, https://www.tandfonline.com/doi/full/10.1080/03071847.2024.2401232.

102 Richterova, Grossfeld, Long, and Bury, 'Russian Sabotage in the Gig Economy Era.'

103 Richterova, Grossfeld, Long, and Bury, 'Russian Sabotage in the Gig Economy Era'; Jones, 'Russia's Shadow War Against the West'.https://www.csis.org/analysis/russias-shadow-war-against-west.

CASE STUDY 3: Espionage trial in the UK

A high-profile espionage trial in the UK exposed a multi-tiered private spy network run by Jan Marsalek, the fugitive former COO of Wirecard, who acted as a freelance broker for Russian intelligence. Marsalek and his Bulgarian associates built an espionage supply chain involving bugged vehicles, cloned IDs, and amateur spies recruited to surveil NATO military installations in Germany. The group also targeted Cristo Grozev, a Bulgarian who worked for Bellingcat, and Roman Dobrokhtov of *The Insider*, whom Moscow had reportedly even considered kidnapping, although the plots were never executed.

The recent sabotage cases throughout Europe and the espionage trial detailed in **Case Study 3**[104] underscore a growing trend: the recruitment of local, previously unaffiliated individuals and amateur sleuths via anonymous digital platforms with little to no oversight.

This volume-based approach has compromised operational quality. Many recruits are clumsy, naïve, and untrained, increasing the risk of exposure. Some appear amateurish, lending credence to the assessment by Richard Moore, former head of the UK's Secret Intelligence Service, that **"Russian intelligence services have gone a bit feral … in some of their behaviour".**[105]

104 Daniela Richterova, 'Putin's Spies for Hire: What the U.K.'s Biggest Espionage Trial Revealed about Kremlin Tactics in Wartime Europe', War on the Rocks, 8 April 2015, https://warontherocks.com/2025/04/putins-spies-for-hire-what-the-u-k-s-biggest-espionage-trial-revealed-about-kremlin-tactics-in-wartime-europe/.

105 'DCIA William Burns and MI6 Chief Richard Moore', Central Intelligence Agency, 7 September, 2024, https://www.cia.gov/static/DCIA_Bill_Burns_MI6_Chief_Richard_Moore_with_FT_Editor_Roula_Khalaf_Transcript.pdf.

Cyber NSAs

By Eginhards Volāns

Key takeaways

- Russia operates one of the world's most advanced offensive cyber ecosystems, built around a diverse set of cyber non-state actors (CNSAs).
- The ties and degree of proximity between these actors and the regime vary considerably, although most are managed through Russian intelligence services.
- While state-controlled hacking groups remain the most capable and frequently used actors at Russia's disposal, hacktivists and cybercriminals are increasingly leveraged.
- Russia's offensive cyber ecosystem is further supported by state-linked research institutes and private IT companies that help to develop essential tools and capabilities.

Introduction

Russia has developed one of the world's most prominent offensive cyber programmes. Its offensive cyber capabilities align closely with its broader strategic culture, which is shaped by a general threat perception rooted in the narrative of a besieged fortress – a mindset that applies to cyberspace as well.[106] **As a result, the Kremlin has regarded cyberspace as a natural arena for geopolitical competition** since the beginning of the internet age. This deeply rooted understanding is best exemplified by two of the earliest and well-known state-backed cyber operations, both linked to the KGB and its successor, the FSB (see **Table 2**).[107]

TABLE 2: Earliest Soviet and Russian cyber operations

The Cuckoo's Egg	**Moonlight Maze**
In 1986, German hacker Markus Hess hacked into US military and industrial systems and sold the acquired information to the KGB. Clifford Stoll, who was involved in capturing Hess, later described the operation and the hunt for Hess in his book *The Cuckoo's Egg*, which gave the operation its name.	One of the first major cyber-espionage campaigns, conducted between 1996 and 1999, targeted US military and government institutions. It was so extensive that an investigation concluded that the stolen documents, if printed out, would triple the height of the Washington Monument. Although it was initially assessed that Russia was behind the attack, there was no hard evidence to support the claim. Only later, through 21st-century investigations, was it discovered that the operation was likely linked to the modern-day, FSB-controlled Turla hacking group.

106 M. J. Kari and Katri Pynnöniemi, 'Theory of Strategic Culture: An Analytical Framework for Russian Cyber Threat Perception', *Journal of Strategic Studies*, Volume 46, Issue 1 (2023): 56–84, https://doi.org/10.1080/01402390.2019.1663411.

107 See Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (Pocket Books, 2005); 'The Hunt for the Dawn of APTs: A 20-Year-Old Attack That Remains Relevant', Kaspersky, 4 April, 2017, https://www.kaspersky.com/about/press-releases/the-hunt-for-the-dawn-of-apts-a-20-year-old-attack-that-remains-relevant.

TABLE 3: Framework of state–CNSA relations[109]

Delegation	Orchestration	Sanctioning
• The state delegates authority to cyber groups, forming a principal-agent relationship. • Agents follow the state's directives closely. • Some agents may act unpredictably, but strict oversight and competition among the groups usually mitigate this. • This type of relationship is ideal for minimising risks and maintaining close control.	• The state partners with ideologically aligned groups by offering support. • At the same time, control is looser than under the delegation framework. • Orchestration depends on shared interests and goals rather than direct orders. • While this approach requires fewer state resources, it also carries greater risk, as some CNSAs might pursue independent agendas.	• The state tolerates but does not directly support the CNSA's activities. • The state turns a "blind eye" to malicious behaviour by the CNSA, often exploiting it to achieve political goals. • This "gentleman's agreement" means that the CNSA deliberately avoids targeting the state, focusing instead on the sponsor state's adversaries.
Example: State-controlled hacking groups controlled by the Russian intelligence services.	**Example:** Pro-Kremlin hacktivist collectives	**Example:** Russian-speaking cybercriminal gangs

Since then, Russia's cyber operations have evolved considerably and are now conducted and supported by a wide range of CNSAs, whose relationships with and degrees of control by the state vary significantly (see **Table 3**).[108] The approximate and indicative scope of Russia's cyber ecosystem is illustrated in **Figure A2**.

For this report, CNSAs are defined as entities controlled by, linked to, aligned with, or influenced by the Kremlin that operate primarily in the cyber domain and leverage cyber power. They take various forms, ranging from state-controlled groups and cybercriminal gangs to lone hacktivists and IT companies contracted by the regime to support its cyber programme.

This chapter maps the CNSAs used by the Russian regime, highlighting their ties to the state, their characteristics, and their value to the Kremlin, while also identifying emerging trends in their role in hybrid threats.

State-controlled hacking groups

Often described in the media as advanced persistent threat (APT) groups,[110] state-controlled hacking groups are almost certainly the most capable cyber assets at the Kremlin's disposal. They are not typical proxies but can instead be viewed as part of the Russian state itself, as the Russian intelligence services (RIS) exercise de facto control over all of them.[111]

However, Russia has never acknowledged their existence and continues to maintain that they have nothing to do with the Russian government.[112] For this reason, state-controlled groups can be defined as a specific sub-category of CNSAs, even though they are deeply embedded within the Russian security apparatus.

Russia's state-controlled cyber groups are highly capable, well-funded, and closely aligned

108 See Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2018).

109 Adapted from Maurer, *Cyber Mercenaries: The State, Hackers, and Power.*

110 Kurt Baker, 'What Is an Advanced Persistent Threat (APT)', CrowdStrike, 4 March 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/.

111 For instance, the US-indicted members of the Sandworm group have been identified as officers of the GRU Military Unit 74455 or the Main Centre for Special Technologies. See Catalin Cimpanu, 'US charges Russian hackers behind NotPetya, KillDisk, OlympicDestroyer attacks', Zdnet, 19 October 2020, https://www.zdnet.com/article/us-charges-russian-hackers-behind-notpetya-killdisk-olympicdestroyer-attacks/.

112 In 2017, Putin stated that pro-Russian hackers targeting the West were not linked to the Russian government but rather acted out of ideological motivations. See 'Putin: khakerami mozhet dvigat' patrioticheskiy nastroi', BBC News Russian Service, 1 June 2017. https://www.bbc.com/russian/news-40118501.

with the Kremlin. As fully state-backed actors, they can access other governmental resources and capabilities to conduct highly sophisticated cyber operations. Given their direct ties to the RIS, their operations can be more easily integrated into Russia's other multidomain information and influence campaigns. For example, they play an important role in election interference,[113] espionage against political opponents, and the use of *kompromat* to enable smear campaigns.[114]

The scope and capabilities of these groups are exemplified by far-reaching operations such as the **2017 NotPetya attack** on Ukraine's financial, government, and energy sectors, often described as "the most devastating cyberattack in history",[115] or the 2020 **SolarWinds attack**, which affected thousands of organisations worldwide, including the US and UK governments, the EU, and NATO.[116] Both operations were carried out by state-backed groups linked to the GRU and the SVR, respectively.

The backgrounds of individual members vary considerably. Some, such as hackers from the FSB-controlled **Turla**[117] group, possess more advanced expertise and formal training in IT.[118] Others, such as those from the GRU-controlled **Sandworm**[119] group, are military officers tasked with conducting cyberattacks as part of their everyday duties.

State-controlled hacking groups are actively employed not only during hybrid threat operations but also in conventional warfare. For example, a GRU-controlled group launched a destructive attack against Viasat's KA-SAT satellite network just hours before Russia's military invasion of Ukraine,[120] demonstrating close coordination with military planning. Since then, state-controlled groups have continued to target Ukraine almost daily, although their focus has shifted from supporting military operations

113 'Russian-Related Threats to the 2020 US Presidential Election', Insikt Group, 3 September 2020, https://go.recordedfuture.com/hubfs/reports/cta-2020-0903.pdf.

114 Compromising material that can be used to blackmail or create negative publicity – a characteristic feature of Russian politics and RIS activities.

115 Andry Greenberg, 'Untold Story of NotPetya, the Most Devastating Cyberattack in History', WIRED, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

116 Saheed Oladimeji, Sean Michael Kerner, 'SolarWinds Hack Explained: Everything You Need to Know', TechTarget, 3 November 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

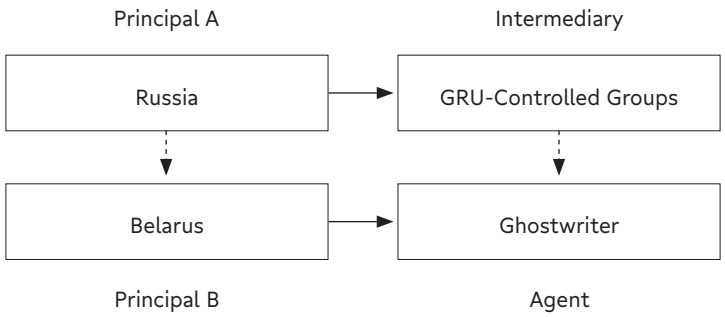
117 Also known as ATK13, Blue Python, G0010, Group 88, Hippo Team, IRON HUNTER, ITG12, KRYPTON, MAKERSMARK, Pacifier APT, Pfinet, Popeye, SIG23, SUMMIT, Secret Blizzard, Snake, TAG_0530, UAC-0003, UAC-0024, UAC-0144, UNC4210, Uroburos, VENOMOUS Bear, WRAITH, Waterbug.

118 Hakan Tanriverdi, Florian Flade, and Lea Frey, 'The Elite Hackers of the FSB', Bayerischer Rundfunk and Westdeutscher Rundfunk, 17 February 2022. https://interaktiv.br.de/elite-hacker-fsb/en/index.html.

119 Also known as APT44, Blue Echidna, ELECTRUM, FROZENBARENTS, G0034, IRIDIUM, IRON VIKING, Quedagh, Seashell Blizzard, TEMP.Noble, TeleBots, UAC-0082, UAC-0113, VOODOO BEAR.

120 Clémence Poirier, 'Hacking the Cosmos: Cyber Operations Against the Space Sector. A Case Study from the War in Ukraine', Cyberdefense Report (Center for Security Studies, ETH Zürich, October 2024) https://css.ethz.ch/en/center/CSS-news/2024/10/hacking-the-cosmos-cyber-operations-against-the-space-sector-a-case-study-from-the-war-in-ukraine.html.

FIGURE 1. Shared agency over the Ghostwriter group



to conducting espionage and enabling information operations.[121]

In addition to directly targeting Russia's adversaries, state-controlled groups often serve as intermediaries between the Russian state and other CNSAs, such as hacktivists and cybercriminals. For example, GRU-controlled groups have established links to several pro-Russian hacktivist collectives,[122] while the FSB's 18th Centre,[123] which oversees groups such as **Gamaredon** and **Callisto**, is known to maintain links to the cybercriminal underground.[124]

Belarus-affiliated groups

Belarus and Russia are believed to cooperate closely in cybersecurity and information operations,[125] including through Russia's use of third-party CNSAs primarily controlled by Belarus. This unique relationship is best exemplified by the **Ghostwriter group**,[126] which is assessed to have links to both Belarus and Russia.[127] Although Ghostwriter operates from Belarusian soil, its operations align with Russia's strategic objectives.

Russian CNSAs, such as GRU-controlled groups, may have supported, trained, or even operated Ghostwriter.[128] As a result, Ghostwriter is used to support the goals of both the Belarusian and Russian regimes.[129] For example, Ghostwriter has targeted Alexander Lukashenko's opposition,[130] hacked news websites and spread disinformation about

121 Allison Pytlak, 'False Alarms: The Role of Cyber Operations in the Russia-Ukraine War', The Henry L. Stimson Center, 29 February 2024, https://www.stimson.org/2024/false-alarms-role-of-cyber-operations-in-the-russia-ukraine-war/.

122 Such as Xaknet, Cyber Army of Russia Reborn and Solntsepek. See A.J. Vicens, Christian Vasquez, 'Sandworm Hackers Targeted Texas Water Facility in 2023, Researchers Say', CyberScoop, 10 April 2024. https://cyberscoop.com/sandworm-apt44-texas-water-facility/.

123 The FSB's 18th Centre oversees groups like Gamaredon, Callisto and possibly Invisimole.

124 Jonathan Greig, 'US Charges Two Russians in Hacks of Government Accounts', The Record, 7 December 2023, https://therecord.media/us-indictment-fsb-alleged-hacking-government-officials.

125 Belarus and Russia are members of the Union State, which facilitates close relations, including intensive military and security cooperation.

126 Also known as DEV-0257, PUSHCHA, Storm-0257, TA445, UAC-0057, UNC1151.

127 'Ghostwriter Campaign', Cardiff University, 2023, 4, https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf.

128 'Ghostwriter in the Shell: Expanding on Mandiant's Attribution of UNC1151 to Belarus', Cyber Threat Analysis, (Insikt Group, March 2022), 3, https://go.recordedfuture.com/hubfs/reports/cta-2022-0318.pdf.

129 Ghostwriter was actively used to target independent Belarusian media and opposition activists before the rigged 2020 presidential election. Its focus shifted towards Russia's adversaries after the invasion of Ukraine, where the group became one of the most active CNSAs targeting Ukraine as well as its allies in the West.

130 Gabriella Roncone et al., 'UNC1151 Assessed with High Confidence to Have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests,' Google Cloud Blog, 15 November 2021, 1, https://cloud.google.com/blog/topics/threat-intelligence/unc1151-linked-to-belarus-government/.

NATO in Poland and Lithuania,[131] supported Russia's military operations,[132] and even targeted Ukrainian refugees.[133] This wide range of targets illustrates the shared and complex agency[134] exercised over the group by both states.[135] **While the dual use of state-controlled hacking groups has been observed only between Russia and Belarus, it sets a troubling precedent.** Similar cooperation between Russia and other Kremlin allies, such as Iran or North Korea, is not evident at present, but cannot be ruled out entirely in the future.

Hacktivists

Modern-day hacktivism differs markedly from its early ideals. What began as a decentralised community of ethical hackers genuinely seeking to protect information freedom has evolved into a more centralised movement aligned with state objectives, often weaponised in state cyber operations (see **Table A2**).[136]

The current wave of hacktivists is more sophisticated, politically aligned, and state-tolerated – or even state-linked – than earlier generations.[137] Pro-Russian hacktivism is now increasingly intertwined with cybercriminal activity, which is changing the nature of the attacks from politically to financially motivated, and making the overall pro-Russian cyber ecosystem ever more complicated.[138]

Russia has been at the forefront of this "hybridisation of hacktivism" since its

131 Dan Sabbagh, 'Russia-aligned Hackers Running Anti-NATO Fake News Campaign – Report', The Guardian, 30 July 2020, https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania.

132 Martin Untersinger, 'Ghostwriter: The Pro-Russian Hackers Crashing the War in Ukraine', Le Monde, 1 May, 2022, 1, https://www.lemonde.fr/en/pixels/article/2022/05/01/ghostwriter-the-pro-russian-hackers-crashing-the-war-in-ukraine_5982121_13.html.

133 Jeff Stone, 'A Propaganda Group Is Using Fake Emails to Target Ukrainian Refugees,' Bloomberg, 22 March, 2023, 1, https://www.bloomberg.com/news/newsletters/2023–03–22/a-propaganda-group-is-using-fake-emails-to-target-ukrainian-refugees.

134 For more information on complex agency in state and proxy relations, see Vladimir Rauta, 'Countering State-Sponsored Proxies: Designing a Robust Policy'.

135 Additionally, other Belarusian-linked groups, assessed as distinct from Ghostwriter, have also been observed. For example, the Winter Vivern group has conducted cyber-espionage activities against European governmental and military targets, while Moustached Bouncer has been spying on foreign diplomats stationed in Belarus. There is no concrete evidence that Russia is linked to these groups as well. See A.J. Vicens, 'Hackers with links to Pro-Russian groups compromised foreign embassies in Belarus, researchers say', CyberScoop, 10 August 2023, 1, https://cyberscoop.com/belarus-hackers-russia-embassies/; Nathan Eddy, 'Russian APT 'Winter Vivern' Targets European Governments, Military', Dark Reading, 17 February 2024, 1, https://www.darkreading.com/cyberattacks-data-breaches/russian-apt-winter-vivern-targets-european-government-military; Matthieu Faou, 'MoustachedBouncer: Espionage Against Foreign Diplomats in Belarus', WeLiveSecurity, 10 August 2023, https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/.

136 James Coker. 'Pro-Russian Hacktivist Group Claims 6600 Attacks Targeting Europe,' Infosecurity Magazine, 5 December 2024. https://www.infosecurity-magazine.com/news/pro-russian-hacktivist-attacks/.

137 Daniel Kapellmann Zafra et al., 'The Global Revival of Hacktivism', Google Cloud Blog, 10 April 2024, https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism.

138 Daryna Antoniuk, 'Russian Hacker Group Killnet Returns with New Identity', The Record, 22 May 2025, https://therecord.media/russian-hacker-group-killnet-returns-with-new-identity.

campaigns against Estonia in 2007[139] **and Georgia in 2008.**[140] Early on, these campaigns revealed that hacktivists play an essential part in Russia's hybrid and conventional military operations and that pro-Russian hacktivists are often linked to RIS.[141]

These trends deepened significantly after Russia's full-scale invasion of Ukraine, during which hacktivists became a key pillar of Russia's cyber power. By the summer of 2023, an estimated 72 pro-Russian CNSAs were involved in the war, the majority of which were hacktivist collectives.[142] Mounting evidence also suggests that at least some of the hacktivist groups targeting Ukraine and its allies, such as the **Cyber Army of Russia Reborn** (CARR), are linked to GRU-controlled groups **APT28** and Sandworm, emphasising the intermediary role of state-controlled hacking groups.[143]

The war in Gaza has also served as a catalyst for the recent surge in state-backed hacktivism. Many pro-Palestinian hacktivists, allegedly backed by Iran, have emerged and established links with pro-Russian groups, further destabilising the cyber domain. This trend is illustrated by the appearance of new alliances, such as CARR's **High Society**[144] and the **Cyber Islamic Resistance's Holy League**.[145]

This growing collaboration between ideologically diverse hacktivist groups may indicate a shift in how hostile states such as Russia and Iran coordinate their operations against a common target (see **Figure 2**).

At the same time, hacktivists have rapidly advanced their capabilities and modus operandi. While their attacks were initially confined to DDoS attacks against countries supporting Ukraine, some groups have since acquired the means to launch destructive cyberattacks

139 James Pamment et al., 'Hybrid Threats: 2007 Cyber Attacks on Estonia', NATO Strategic Communications Centre of Excellence (NATO StratCom CoE, June 2019), https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

140 Alexander Melikishvili, 'The Cyber Dimension of Russia's Attack on Georgia', *Eurasia Daily Monitor*, Volume 5, No. 175 (12 September 2008), https://jamestown.org/program/the-cyber-dimension-of-russias-attack-on-georgia/.

141 John Leyden, 'Russian Spy Agencies Linked to Georgian Cyber-Attacks', The Register, 23 March 2009, https://www.theregister.com/2009/03/23/georgia_russia_cyberwar_analysis/.

142 Cyber Know, 'Update 24. 2023 Russia-Ukraine War — Cybertracker', Medium, 20 July 2023. https://cyberknow.medium.com/update-24–2023-russia-ukraine-war-cybertracker-20-july-ec64cfef38a0.

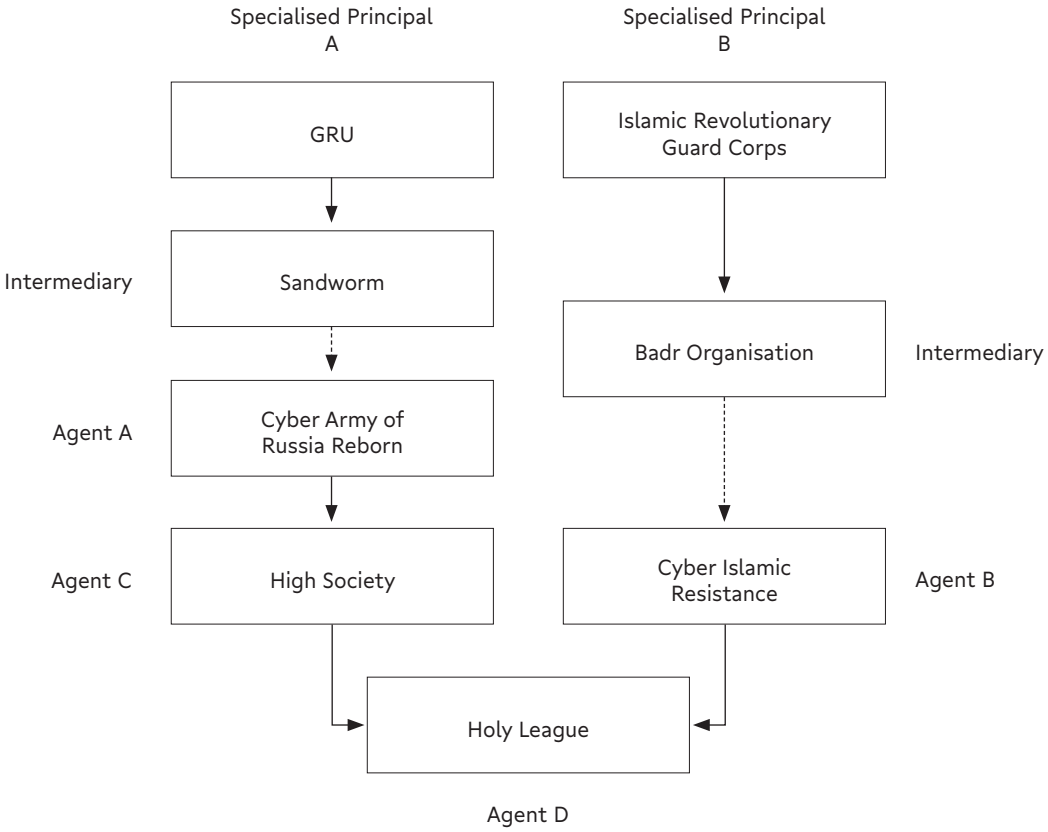
143 'Hacktivists Collaborate with GRU-sponsored APT28', Google Cloud Blog, 23 September 2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions.

144 Samiksha Jain, 'High Society, New Alliance Linked to Cyber Army of Russia', The Cyber Express, 6 May 2024, https://thecyberexpress.com/cyber-army-of-russia-affiliate-high-society/.

145 CARR is allegedly linked to the GRU-controlled group Sandworm, while Cyber Islamic Resistance has claimed to have received training from the IRGC-aligned Badr organisation. See Paul Shread, 'Holy League Hacktivists Uniting Against France', The Cyber Express, 12 December 2024. https://thecyberexpress.com/holy-league-hacktivists-uniting-against-france/; Tom Ball, 'British Infrastructure Security Targeted by Pro-Russian and Palestinian Hacktivists', The Times, 6 April 2025, https://www.thetimes.com/uk/crime/article/british-infrastructure-security-pro-russian-palestinian-hacktivists-509m9w3gq.

FIGURE 2. Emerging hacktivist alliances

Some hacktivist groups appear to have created new, indirect links between hostile state actors. Since 2024, for instance, the *Holy League*, an alliance of pro-Russian and pro-Palestinian hacktivists, has routinely targeted the Western allies of Israel and Ukraine. Although the alliance itself lacks direct state ties, some of its members reportedly maintain connections to both the GRU and the Islamic Revolutionary Guard Corps (IRGC). These links are indirect and possibly mediated through groups such as the GRU's Sandworm or the IRGC-linked Badr Organisation.



targeting water and energy infrastructure.[146] Others have developed cyberespionage capabilities[147] or hijacked satellite television broadcasting to support Russia's information operations.[148] Some hacktivists have become a propaganda staple in Russia, often interviewed by Russian media and spreading pro-Russian narratives to the public.[149]

The increased state reliance on hacktivists is justified by their ability to provide greater deniability and legitimacy than state-controlled groups. First, they are used to suggest that the attacks are conducted by ideologically motivated individuals without any state links or backing. Second, the notion of an independent community supporting the state's strategic

146 'Russian Hacktivists Target Energy and Water Infrastructure', Cyble, 6 December 2024, https://cyble.com/blog/russian-hacktivists-target-energy-and-water-infrastructure/.

147 'Russia-Based Hacker Group 'XakNet' Infiltrates Ukraine Finance Ministry', The Cyber Express, 26 May 2023, https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

148 'Russia Attacks Ukraine's Satellite TV, Dozens of Channels Experience Issues', Ukrainska Pravda,17 April 2024, https://www.pravda.com.ua/eng/news/2024/04/17/7451697/.

149 Roman Kildyushkin, 'Lider khakerskoy gruppy Phoenix rasskazal, kak i skol'ko zarabatyvayut russkie khaktivisty', Gazeta, 24 February 2023. https://www.gazeta.ru/tech/news/2023/02/24/19822867.shtml.

CASE STUDY 4: Intricate ties between the FSB and cybercriminals

The complex relationship between cybercriminals and the RIS is exemplified by Dmitry Dokuchaev, a former hacker hired by the FSB's 18th Centre. In 2014, the US accused Dokuchaev of hacking Yahoo, an operation conducted using outsourced cybercriminals. Despite his role in the FSB, he was charged with treason in 2016, after being accused of passing classified information to the CIA. Dokuchaev was believed to have recruited the hacktivist collective Shaltai Boltai without FSB authorisation. This may have led to friction between Dokuchaev and other FSB branches and his eventual downfall.

objectives is ideal for projecting its image as a global cyber power with international support. This is particularly true of pro-Russian hacktivists, who often publicly exaggerate the effectiveness and scope of their attacks.[150]

Hacktivism is no longer just a side phenomenon – it has become integral to modern cyber threats and is actively exploited by hostile states. As these groups become more powerful and acquire more destructive capabilities, the risk of unintended escalation will likely increase, as state backers risk losing control over the groups they empower.

Cybercriminals

The Russian cybercriminal scene has long been highly active and prominent. This is mainly due to the strong technical education system, a legacy of the Soviet Union, and to the collapse of state funding for research and universities in the 1990s, which, together with the rapid and unregulated development of Russia's internet segment, created ideal conditions for cybercriminals to thrive.[151]

These groups have developed impressive destructive capabilities, as demonstrated by the 2021 attacks on the US Colonial Pipeline[152] and Brazil's meat processing company JBS.[153] Both attacks were carried out by Russian-speaking cybercriminal groups DarkSide and REvil, and resulted in significant fuel shortages and disruptions to the meat supply chains in the US. Their prominence is likely growing, as recent research shows that 69% of global ransomware proceeds are linked to Russian-speaking groups.[154]

In the 1990s and 2000s, the RIS actively exploited the newly established cybercriminal "talent pool", recruiting hackers either through direct employment or by blackmailing them into working for the Kremlin. This was particularly true of the FSB, whose 18th Centre is formally tasked with countering cybercrime.[155] As a result, the FSB cemented itself as the service with the most extensive links to the cybercriminal underworld (see **Case Study 4**).[156]

150 James Coker, 'Pro-Russian Hacktivist Attacks Surge in Q1 2024', Infosecurity Magazine, April 9, 2024. https://www.infosecurity-magazine.com/news/pro-russian-hacktivist-attacks/.

151 Alec Jackson, 'How the Collapse of the Soviet Union Made Russia a Great Cyber Power', The Cyber Defense Review, Volume 9, Issue 1, 2024, 101–116. https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Spring/Jackson_CDRV9N1-Spring-2024.pdf.

152 'The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years', Cybersecurity and Infrastructure Security Agency, 7 May 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

153 Brian Menegus, 'World's largest meat supplier grinds to a halt after cyberattack', The Verge, 1 June 2021. https://www.theverge.com/2021/6/1/22463621/jbs-cyberattack-russia-largest-meat-supplier.

154 'New TRM Report Reveals Russian-Speaking Groups Dominate Ransomware', TRM Labs, 25 July 2024, https://www.trmlabs.com/resources/blog/new-trm-report-reveals-russian-speaking-groups-dominate-ransomware.

155 'Pervaya sluzhba i Tsentr informatsionnoy bezopasnosti', Dossier.Center, https://fsb.dossier.center/1s/.

156 'Figuriruyushchiy v dele o gosizmene sotrudnik FSB v proshlom byl khakerom', RBC, 27 January 2017, https://www.rbc.ru/society/27/01/2017/588b07ba9a79472f625421ea; 'US Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts', US Department of Justice, 15 March 2017, https://www.justice.gov/archives/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-

While relations between Russia and cybercriminals have historically remained informal, these ties now appear increasingly "direct and explicit".[157] Both Microsoft and Google have observed an increasing overlap between Russia's objectives and cybercriminal activity, with Google noting that "Russia has drawn on criminal capabilities to fuel the cyber support for its war in Ukraine".[158] Similarly, the Insikt Group has concluded that cybercriminals and the RIS have a "tacit understanding" and that their relationships are "established and systematic".[159]

The Kremlin places high value on the services that cybercriminals can provide to the Russian state. These services extend beyond offering additional, deniable destructive cyber power to include expertise in illicit financing schemes, which the regime needs to circumvent sanctions (the role of cybercriminals is discussed in more detail in the chapter on EFNSAs).

Their value in the eyes of the regime is best exemplified by recent prisoner exchanges involving several notorious cybercriminals. During a 2024 prisoner exchange between Russia and the West, Moscow secured the release of two prominent cybercriminals, Roman Seleznev and Vladyslav Klyushin.[160] Seleznev was a hacker with close ties to the regime,[161] while Klyushin was an IT company executive with links to the state.[162] Another cybercriminal, **Aleksander Vinnik**, was released in 2025,[163] and Russian authorities also facilitated the extraction of cybercriminal **Oleg Nefedov** after his detention in Armenia.[164]

conspirators-hacking-yahoo-and-millions; Andrew Roth, 'The FBI Just Indicted a Russian Official for Hacking – but Why Did Russia Charge Him with Treason?', Washington Post, 16 March 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/03/16/the-fbi-just-indicted-a-russian-official-for-hacking-but-why-did-russia-charge-him-with-treason/.

157 Tom Uren, 'Russia's Cybercriminals and Spies Are Officially in Cahoots', Lawfare, 30 May 2025, https://www.lawfaremedia.org/article/russia's-cybercriminals-and-spies-are-officially-in-cahoots.

158 See 'Cybercrime: A Multifaceted National Security Threat', Google Cloud Blog, 18 March 2024; 'Microsoft Digital Defense Report 2024', (Microsoft, 2024), 17, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat.

159 'Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine', Insikt Group (Recorded Future, January 2023), https://go.recordedfuture.com/hubfs/reports/cta-2023-0131.pdf.

160 'Russia exchanges spies for political prisoners: Gershkovich, Kara-Murza, Whelan, Yashin, Kurmasheva, Chanysheva, Orlov released', The Insider, 1 August 2024, https://theins.ru/en/news/273542.

161 Seleznev's father, Valeriy, is a member of the Russian State Duma.

162 Klyushin's company, M-13, developed the media monitoring tool Katyusha, widely used by Russian state institutions.

163 Vinnik's cryptocurrency company BTC-e was assessed to have been used by the GRU-controlled APT28 group to finance operations against the US Democratic National Committee in 2015–2016. See Filip Lebedev and Mark Trevelyan, 'Who Is Alexander Vinnik, the Russian Prisoner Being Traded for American Marc Fogel?', Reuters, 12 February 2025, https://www.reuters.com/world/europe/who-is-alexander-vinnik-russian-prisoner-being-traded-american-marc-fogel-2025-02-12/.

164 Nefedov was a leader of the ransomware-as-a-service gang Black Basta. See Kristina Beek, 'Black Basta, Conti, the FSB & the Leaked Chat Logs That May Link Them', Dark Reading, 18 March 2025. https://www.darkreading.com/threat-intelligence/black-basta-league-russian-officials-chat-logs.

Cyber enablers

Various CNSAs are used to support the previously discussed state-controlled hacking groups by developing custom cyber tools or providing information essential for conducting cyber operations.

Russia's cyber programme relies heavily on private IT companies. These firms do not carry out cyberattacks directly but assist state hackers through software development. Examples include companies such as **NTC Vulkan**, which, according to leaked internal documents, has developed tools for the GRU-controlled **Sandworm** group.[165] Similarly, leaked documents from IT company **SyTech** exposed its links to the FSB.[166] The US Treasury Department has also acknowledged the close relationship between the RIS and IT developers by sanctioning at least six Russian companies.[167] **The FSB has a particular advantage in establishing relations with the private IT sector**, as it is responsible for issuing information security certificates and can therefore exert additional influence over private entities.[168]

In addition to software development, some companies are also used to recruit talented individuals. For example, Positive Technologies hosts hacker competitions such as *Hacker Days* and *The Standoff*, which the RIS can use to identify and approach young hackers for recruitment into state-controlled groups.[169]

Some foreign companies have also been contracted to support Russia's cyber programme. For example, the Scientific Research Institute Kvant, known for its ties to the FSB's 16th Centre,[170] contracted Milan-based company Hacking Team to purchase software capable of remotely accessing cell phones and computers.[171]

Most research centres in Russia also maintain ties to the RIS. Some act as intermediaries between the RIS and private IT companies, while others have re-established themselves as private entities.[172] Many of these research centres date back to the Soviet era or even earlier, when they established strong ties to

165 Alden Wahlstrom et al. 'Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan', Google Cloud Blog, 30 March 2023. https://cloud.google.com/blog/topics/threat-intelligence/cyber-operations-russian-vulkan.

166 Catalin Cimpanu, 'Hackers Breach FSB Contractor, Expose Tor-Deanonymization Project', ZDNet, 20 July 2019. https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/.

167 'Treasury Sanctions Russia with Sweeping New Sanctions Authority', US Department of the Treasury, 15 April 2021. https://home.treasury.gov/news/press-releases/jy0127.

168 'Kak ustroeny sertifikaty bezopasnosti dlya operatsionnykh sistem', CNews, March 28 2024, https://market.cnews.ru/articles/2024–03–26_kak_ustroeny_sertifikaty_bezopasnosti.

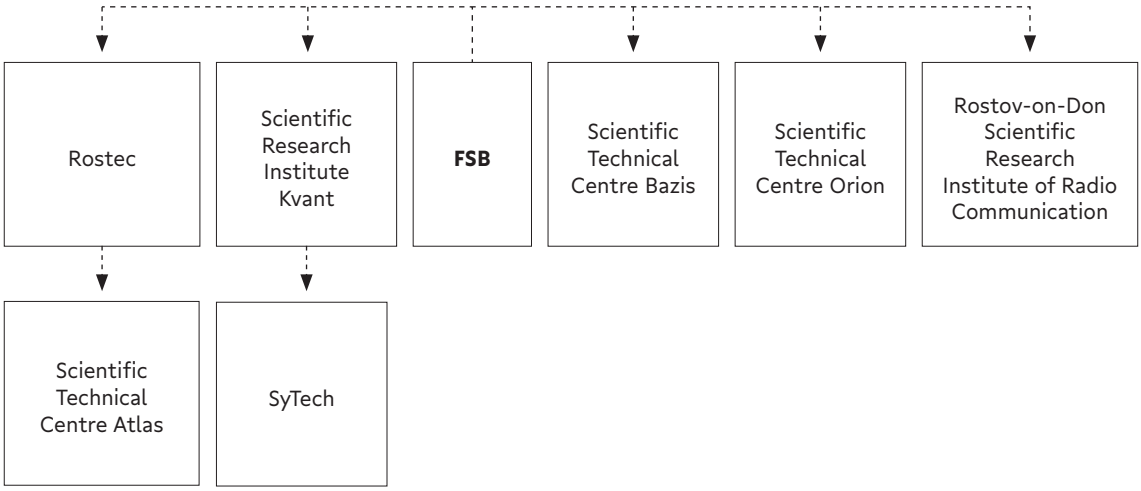
169 Andrey Soldatov and Irina Borogan, 'Russian Cyberwarfare: Unpacking the Kremlin's Capabilities', Center for European Policy Analysis, 8 September 2024, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

170 The FSB's 16th Centre is in charge of the notorious Turla group.

171 Daniil Turovskiy, 'Rossiyskie Vooruzhennye Kibersily', Meduza, 7 November 2016. https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily.

172 For example, the IT company SyTech, a contractor for the FSB, was established with the help of the FSB-linked research centre Kvant. See Andrei Soldatov, 'Nauchno-Issledovatelskaya Imperiya FSB', Agentura, 11 July 2023, https://agentura.ru/investigations/nauchno-issledovatelskaja-imperija-fsb/.

FIGURE 3. Selected FSB-linked research facilities and IT companies[175]



the KGB or the Russian military. In many cases, these links remain intact.[174] A clear example of these historical ties is the **Central Scientific Research Institute of Chemistry and Mechanics**, established at the end of the 19th century to support Russia's military–industrial complex even before the 1917 Bolshevik Revolution. It continues to operate today, developing custom cyber tools for Russian hackers.[175]

173 Adapted from Soldatov, 'Nauchno-Issledovatelskaya Imperiya FSB'.

174 See Soldatov, 'Nauchno-Issledovatelskaya Imperiya FSB'.

175 'Triton Attribution: Russian Government-Owned Lab Most Likely Built Tools', Google Cloud Blog, 23 October 2018, https://cloud.google.com/blog/topics/threat-intelligence/triton-attribution-russian-government-owned-lab-most-likely-built-tools.

Propaganda and disinformation NSAs

By Eginhards Volāns

Key takeaways

- Propaganda and disinformation non-state actors (PDNSAs) form the backbone of the Kremlin's influence over domestic and foreign audiences, as they are cost-effective and can achieve a high impact without direct confrontation.
- While traditional media remains important for reaching the domestic population, social media, influencers, and other unconventional actors are increasingly used to advance Russia's goals abroad.
- Since 2022, PDNSA activities have become increasingly outsourced and covert, mimicking genuine and legitimate actors, which makes them difficult to identify, track, and attribute to Russia.
- PDNSA operations are increasingly backed by various private-sector entities, such as PR agencies and IT companies, which are necessary for setting up the infrastructure and further blurring the lines between PDNSAs and the Russian regime.

Introduction

Since its invasion of Ukraine, Russia has significantly intensified its information confrontation[176] with the West. The Kremlin has sought to undermine Western support for Ukraine[177] and, more recently, to influence democratic processes in several Western countries.[178] It has also worked to weaken Western interests in other regions, particularly in the so-called Global South.[179] These trends have been acknowledged by experts and democratic leaders alike.[180]

Russia's reliance on propaganda and disinformation to exert influence and weaken

176 Information confrontation is a concept in which Russia views the information domain as a battlefield, where it can use propaganda and disinformation to weaken opponents and protect its interests. The text uses the term information confrontation to capture a broader range of hostile activities than those covered by information or psychological operations. See Michelle Grisé et al., 'Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation', RAND Corporation Report, (RAND Corporation, 2022), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA198-8/RAND_RRA198-8.pdf.

177 Nicholas Vinocur, Pieter Haeck, and Eddy Wax, 'Russian influence scandal rocks EU', Politico, 29 March 2024. https://www.politico.eu/article/voice-of-europe-russia-influence-scandal-election/.

178 The most recent examples include elections in the US, Moldova, Romania, Croatia and Germany. See Julian E. Barnes and Steven Lee Myers, 'Russia Disinformation and the Election', The New York Times, 15 May 2024, https://www.nytimes.com/2024/05/15/us/politics/russia-disinformation-election.html; Vitalie Calugareanu, 'Moldovan Police Explain How Russia Meddled in Recent Polls', Deutsche Welle, 30 October 2024, https://www.dw.com/en/moldovan-police-explain-how-russia-meddled-in-recent-polls/a-70636678; Seb Starcevic, 'Russian Bots Boosted NATO Critic Ahead of Croatian Election, Researchers Say', Politico, 9 January 2025, https://www.politico.eu/article/russia-bots-nato-croatia-election-presidential-candidate-eu-donald-trump-zoran-milanovic-campaign/; Riham Alkousaa, 'Germany Warns of Russian Disinformation Targeting Election', Reuters, 21 February 2025, https://www.reuters.com/world/europe/germany-warns-russian-disinformation-targeting-election-2025-02-21/.

179 Dominik Presl, 'Russia is Winning the Global Information War', RUSI Commentary, 7 May 2024, https://rusi.org/explore-our-research/publications/commentary/russia-winning-global-information-war.

180 'G7 says Russia finding covert efforts to undermine elected governments', Reuters, 17 January 2025. https://www.reuters.com/world/europe/g7-says-russia-finding-covert-efforts-undermine-elected-governments-2025-01-17/.

TABLE 4. Institutionalisation of Russian propaganda and disinformation[181]

Crowdsourcing model	Outsourcing model	Insourcing model
• Emerged during the Medvedev era due to limited government resources and expertise. • Focused on domestic rather than external audiences. • Aimed to promote a positive state image through initiatives such as *Russia Without Fools* and *Active Citizen*.	• Emerged during the Medvedev-Putin era as crowdsourcing limitations shifted the focus to outsourcing. • Early domestic projects included *Nashi* for internal audiences and the Internet Research Agency for external ones. • Trolls, computational propaganda, and hacker groups became key tools in Russia's information-confrontation strategies.	• Emerged after the constitutional referendum to centralise and professionalise propaganda and disinformation operations. • ANO Dialog integrated vertical state control into horizontal public networks. • Although it appears to be outsourced, this model is actually insourced and tightly controlled by the state. • Since 2022, the focus has shifted to external audiences, using microtargeted, marketing-based tactics.

adversaries is nothing new. During the Cold War, this practice was commonly referred to as "active measures" and was widely employed by the KGB.[182] Modern-day Russia has largely adapted these Soviet-era tactics, enhancing them through recent technological advances.

Russia's hostile activities in the information domain have evolved over time, becoming more professional, unified, and tightly controlled by the Kremlin[183] – and therefore even harder to detect and counter (see **Table 4**). At the centre of these activities lie NSAs, whose ties to the Kremlin are often challenging to prove, enabling them to evade direct sanctions while claiming freedom of the press and exploiting other democratic values. As a result, greater clarity is required on this issue.

While most NSAs wield some form of media power – particularly those discussed in the chapter on 'Social and political NSAs', this chapter focuses on those that are primarily active in the information domain, collectively referred to as PDNSAs. They take various forms, ranging from lone influencers to coordinated troll factories, from fringe media projects to state-of-the-art media conglomerates. Their connections to the Russian state range from informal and blurred to almost directly state-controlled, all while presenting themselves as impartial and independent.

This chapter defines several distinct sub-categories of PDNSAs and clarifies the blurred lines between them and the Russian state, highlighting their roles, characteristics, and value to the Kremlin.

181 Adapted from G. Asmolov, 'Propaganda v setevoy srede'.

182 Ivo Juurvee, 'The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox', Hybrid CoE Strategic Analysis 7 (Hybrid CoE, April 2018), 3. https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-7-April.pdf.

183 Grigory Asmolov, 'Propaganda v setevoy srede: kak menyalas propaganda v epokhu sotsialnykh media i v usloviyakh voyny', Re: Russia, 5 April 2024. https://re-russia.net/expertise/714/.

Traditional media

Traditional media – including television, radio, print, and even books – have been the primary instruments for controlling narratives within Russia for decades. Although formally independent, these outlets are often managed by conglomerates loyal to the Kremlin and either rely on state funding or have strong ownership ties to the government. For instance, **NMG**,[184] one of Russia's largest media companies, is de facto controlled by **Yuri Kovalchuk**, a close associate of Putin.[185]

Today, almost all Russian traditional media outlets act as appendages of the Russian state. Russia's 2025 budget plans include record-high weekly spending of approximately 2.6 billion roubles[186] on propaganda, demonstrating the importance placed on this tool.[187] Despite their declining popularity,[188] most of the spending is dedicated to Russia's TV channels, which remain central to the regime's propaganda ecosystem.

TV has also proved to be an effective means of reaching Russia's compatriots abroad. This poses a significant threat to countries with large Russian communities, particularly the Baltic states. For instance, a 2018 study found that in Latvia, where 23.4% of the population are ethnic Russians,[189] around 82% of non-ethnic Latvians watched Russian TV daily.[190] In addition, some channels, such as **Perviy Baltiyskiy Kanal**, have been explicitly designed to influence Russian-speaking audiences abroad.

Although Russian TV is now blocked in the Baltics, it has adapted and found covert ways to continue influencing audiences, essentially becoming even harder to detect, track and counter. For instance, Latvian journalists have reported that Russian TV content remains

184 Adapted from G. Asmolov, 'Propaganda v setevoy srede'.
185 Natsionalnaya Media Gruppa – NMG.
186 About 24 million euros.
187 The significance of traditional media was particularly noticeable during Putin's consolidation of power in the early 2000s, which began with the takeover of the NTV headquarters. After that, the crackdown on opposition media intensified after the Bolotnaya protests in 2011–2013. Following the invasion of Ukraine, the Kremlin gained complete control over Russia's information space, using it as a catalyst to ban or oust the remaining opposition media. See Sharon LaFraniere, 'Russian Network Seized in Raid', The Washington Post, 15 April 2001, https://www.washingtonpost.com/archive/politics/2001/04/15/russian-network-seized-in-raid/e9679fb0–31cb-4b9c-b07f-204b488f40ad/; Ksenia Luchenko, 'Vnutri i snaruzhi tsenzury: rossiiskii medialandshaft cherez dva goda posle nachala voiny', Re:Russia, 22 May 2024, https://re-russia.net/expertise/0154/.
188 Viktor Vladimirov, 'Prokremlevskie media teryayut auditoriyu', Golos Ameriki, 10 January, 2025, https://www.golosameriki.com/a/russian-media-audience-fall/7932574.html.
189 Central Statistical Bureau of Latvia, 'Population by Ethnicity in Regions, State Cities and Municipalities at the Beginning of the Year 2012–2024', https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__POP__IR__IRE/IRE031/table/tableViewLayout1/.
190 Visvaldis Valtenbergs et al., 'Krievijas ietekme Latvijas informatīvajā telpā', Saeimas Analītiskā Dienesta ziņojums, (Latvijas Republikas Saeima, Janvāris 2018), 10, https://www.saeima.lv/petijumi/Krievijas_ietekme_Latvijas_informativaja_telpa_elektroniski.pdf.

accessible via YouTube and various mobile apps and continues to attract local viewers.[191]

The RT network is an essential tool for global influence, capable of reaching audiences beyond the Russian diaspora. Although formally managed by an "autonomous non-profit organisation" (NPO),[192] RT is entirely funded and controlled by the Russian government.[193] RT has significantly expanded its operations post-2022 and is known to operate bot networks and hundreds of covert websites.[194] Moreover, the US Department of State notes that RT has developed cyber capabilities and is engaged in military procurement activities,[195] making it a highly versatile asset for the Russian regime.

Russian traditional media increasingly targets audiences in the Global South as well. Projects such as **TV BRICS** are aimed at establishing networks between journalists, training new journalists and spreading pro-Kremlin narratives worldwide.[196] Additionally, media outlets such as Venezuela's TeleSur work closely with RT to amplify and legitimise narratives in Latin America.[197]

The international influence of the Russian press and radio is limited, although exceptions exist in countries with Russian communities. For example, the New York-based World Association of Russian Press supervises the development of Russian-language newspapers in around 80 countries.[198] Additionally, Russia has used **Radio Sputnik** to disseminate propaganda to international audiences through independent stations in the West. In Latvia, for instance, Sputnik shows were aired daily on the local Avto Radio, owned by a local pro-Kremlin politician.[199]

191 'Aizliegtais paņēmiens: Krievijas kanāli Latvijā oficiāli slēgti, bet YouTube skaties, ko vēlies', Latvijas Sabiedriskais Medijs, 16 September 2024, https://www.lsm.lv/raksts/zinas/latvija/16.09.2024-aizliegtais-panemiens-krievijas-kanali-latvija-oficiali-slegti-bet-youtube-skaties-ko-velies.a568955/.

192 ANO TV-Novosti.

193 'Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem', Global Engagement Center Special Report (US Department of State, January 2022), 7, https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf.

194 Bret Schafer et al., 'The Russian Propaganda Nesting Doll: How RT is Layered Into the Digital Information Environment', Alliance for Securing Democracy Report (German Marshall Fund, May 2024), 5, https://securingdemocracy.gmfus.org/wp-content/uploads/2024/05/Laundromat-Paper.pdf.

195 'Alerting the World to RT's Global Covert Activities', US Department of State, 13 September 2024, https://www.state.gov/alerting-the-world-to-rts-global-covert-activities/.

196 Peter Benzoni, Larissa Doroshenko, and James Conway, 'What Is TV BRICS? The Sanctions-Linked, Russia-Backed Influence Broker', GMFUS, 11 February 2025, https://www.gmfus.org/news/what-tv-brics-sanctions-linked-russia-backed-influence-broker.

197 Mark A. Green, 'Latin America Loves Russia Today Publication', Wilson Center, 18 July 2023, https://www.wilsoncenter.org/blog-post/latin-america-loves-russia-today-publication.

198 Andrey Kuzichkin, Monika Hanley, 'Russian media landscape: Structures, mechanisms, and technologies of information operations', NATO Strategic Communications Centre of Excellence Report, (NATO StratCom CoE, June 2021), 35. https://stratcomcoe.org/pdfjs/?file=/publications/download/Report_Russian_Media_Landscape_2021.pdf?zoom=page-fit.

199 'VDD Arestētais 'Sputnik Lietuva' Redaktors Kasems: Meloju Naudas Dēļ', TV3, 11 September 2023, https://zinas.tv3.lv/latvija/neka-personiga/video/vdd-arestetais-sputnik-lietuva-redaktors-kasems-meloju-naudas-del/.

Similarly, Sputnik continued to reach US audiences through Missouri stations even after 2022.[200]

Digital media

Russia increasingly relies on proxy websites that masquerade as independent outlets, while social media platforms are often manipulated or coerced to amplify pro-Russian messages.

State entities, such as the RIS, along with NPOs, think tanks and PR agencies, play a key role in creating and managing various digital media projects. For instance, the GRU operates the **Institute of the Russian Diaspora**, which manages proxy websites such as **InfoRos**,[201] an effort that has led to the creation of approximately 1,300 other Russian-language websites alone.[202] Meanwhile, the SVR is known to operate the **Strategic Culture Foundation**[203] and to use its front organisation, **Myrotvorets**, to carry out other covert operations in Europe,[204] while the FSB orchestrates websites such as **NewsFront** and **SouthFront**.[205]

Russian propaganda has also been advanced by entire social media platforms. Odnoklassniki and **VK**, both under direct Kremlin influence, promote Russian propaganda while censoring criticism of the Kremlin. As a result, countries with large Russian-speaking user bases, such as the Baltic states, have restricted access to these platforms.[206]

Concerns have likewise been raised about Russia's influence over **Telegram**, which has gradually evolved into a hub for Russian propaganda.[207] Russia has used Telegram to

200 Katherine Gypson, 'Two US Radio Stations End Russian-backed 'propaganda' Programming', Voice of America, 16 October 2024, https://www.voanews.com/a/two-us-radio-stations-end-russian-backed-propaganda-programming/7824863.html.

201 Michael Weiss, ed., 'Aquarium Leaks: Inside the GRU's Psychological Warfare Program', Free Russia Foundation Report (Free Russia Foundation, 2020), 8, https://thinktank.4freerussia.org/wp-content/uploads/2020/12/AquariumLeaks-EN-Web-1.pdf.

202 'The GRU's Galaxy of Russian-Speaking Websites', OpenFacto Report (OpenFacto, January 2022), https://drive.google.com/file/d/1xIbx6ZTyBuQB_4iZ9JNureHJgHYu3Di0/view.

203 'Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors,' US Department of the Treasury, 3 March 2022, https://home.treasury.gov/news/press-releases/jy0628.

204 Roman Dobrokhotov, Hristo Groziev and Michael Weiss, 'Soobrazheniyami morali i nravstvennosti prenebrech: kak SVR organizuet dezinformatsionnye kampanii na Zapade', The Insider, 4 July 2024, https://theins.ru/politika/272852.

205 'Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm', US Department of Justice, 9 July 2024, https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners.

206 'Russian social media networks VKontakte, Odnoklassniki to be blocked in Latvia', Latvijas Sabiedriskais Medijs, 12 May 2022, https://eng.lsm.lv/article/features/media-literacy/russian-social-media-networks-vkontakte-odnoklassniki-to-be-blocked-in-latvia.a456465/.

207 'Another battlefield: Telegram as a digital front in Russia's war against Ukraine', Atlantic Council's Digital Forensics Lab, 7 June 2024, https://dfrlab.org/2024/06/10/another-battlefield-russian-telegram/.

CASE STUDY 5: Telegram

Telegram was launched in 2013 by the Durov brothers after they were forced to sell their previous project, the immensely popular social network VKontakte, to pro-Kremlin oligarch Alisher Usmanov. The app quickly gained popularity and was seen by the Russian population as one of the last spaces free from the regime's censorship.

In 2017, the Russian government targeted Telegram to gain access to its encryption keys. Telegram's refusal to cooperate led to the app being banned in Russia in 2018. However, the ban was effectively unenforceable, as Russia lacked the technology to block access at that time.

By 2020, the Russian regime had de facto lifted the ban and altered its strategy to exploit the platform instead. Russian politicians, state institutions, and media outlets became active users of Telegram, and covert propaganda networks were created. During the COVID-19 pandemic, Telegram's popularity expanded outside Russia, particularly within conspiracy theory communities. Following Russia's invasion of Ukraine, Telegram became one of the main hubs for Russian propaganda.

target Ukraine,[208] Moldova[209] and Georgia,[210] among others. While there is no solid evidence of direct ties to the Kremlin, the platform's owner, **Pavel Durov**, frequently visits Russia and maintains business associations with individuals linked to the RIS, suggesting potential cooperation with the Russian government.[211]

Influencers

The Kremlin relies heavily on traditional opinion leaders, including journalists, political scientists and historians, to lend legitimacy to its narratives. Some are explicitly tasked with influencing foreign audiences in post-Soviet countries, where the Presidential Administration (PA) has developed networks of professional influencers. Under the guidance of the RIS, these figures are used to organise protests, establish pro-Russian organisations, and engage in media manipulation.[212] Leaked emails from Kremlin ideologue **Vladislav Surkov** explicitly highlight the significance of influencers, indicating that maintaining such networks is central to Russia's foreign interference efforts.[213]

Beyond the post-Soviet space, international audiences are also being targeted. British national **Graham Phillips**[214] and Australian **Simeon Boikov**[215] exemplify Russia's use of

208 Ivan Makridin, 'How Telegram Became the Hub of Russian Propaganda', Coda Story, 17 April 2024. https://www.codastory.com/newsletters/how-telegram-became-the-hub-of-russian-propaganda/.

209 Givi Gigitashvili, Victoria Olari, 'Moldova in the digital crosshairs of anonymous, pro-Russian Telegram channels', Atlantic Council's Digital Forensics Lab, 12 April 2024, https://dfrlab.org/2024/04/12/moldova-digital-crosshairs-pro-russian-telegram-channels/.

210 Givi Gigitashvili, 'Russian-language Telegram channels foment tensions in Georgia', Atlantic Council's Digital Forensics Lab, 1 May 2024. https://dfrlab.org/2024/05/01/russian-language-telegram-channels-foment-tensions-in-georgia/.

211 See Nikita Kondratev, Egor Feoktistov, and Anastasia Korotkova, 'Pavel Durov Has Visited Russia More Than 50 Times Since His 'Exile' in 2014', Important Stories, 27 August 2024, https://istories.media/en/news/2024/08/27/pavel-durov-has-visited-russia-more-than-50-times-since-his-exile-in-2014/; Roman Anin and Nikita Kondratyev, 'Telegram, the FSB, and the Man in the Middle', iStories, 10 June 2025, https://istories.media/en/stories/2025/06/10/telegram-fsb/.

212 'Pribaltika: Issledovanie vliyaniya Rossii v stranakh Pribaltiki', Dossier Center, 25 November 2020, https://dossier.center/pribaltika/.

213 Alya Shandra and Robert Seely, 'The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine', RUSI Report, (RUSI, July 2019), 80, https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf.

214 'Graham Phillips: the civil servant-turned-Putin propagandist', The Week, 21 April 2022, https://theweek.com/news/world-news/russia/956479/who-is-graham-phillips-former-civil-servant-putin-propagandist.

215 Sean Nicholls, Jeanavive McGregor, Mary Fallon, and Alex Palmer, 'Meet the Russian Patriots Making Their Presence Felt in Australia', ABC News, 14 February 2021, https://www.abc.net.au/news/2021–02–15/four-corners-putin-russia-influence/13139628.

foreign nationals to whitewash its military aggression against Ukraine. Western nationals working for the Kremlin often have personal or ideological ties to Russia, motivating them to spread Kremlin propaganda. For instance, Boikov's parents are ethnic Russians, while Phillips was exposed to pro-Russian views while living in Eastern Ukraine.

A broader strategy can be identified in Russia's reliance on local networks to legitimise pro-Russian narratives and shape public opinion abroad. This includes funding popular American right-wing influencers through **Tenet Media**,[216] and hiring South African influencers through a local influencer marketplace to spread anti-Zelenskyy messages.[217]

Influencers participating in the Kremlin's operations are often contracted through regime-linked advertising companies such as **AdNow**, which manipulated bloggers to spread disinformation during the COVID-19 pandemic[218] and was involved in interference in the 2024 Romanian presidential election.[219]

Since 2022, Russia has increasingly relied on military bloggers (*voenkory*)[220] to shape narratives about the war. These figures have gained significant prominence within Russia – meeting with Putin and receiving medals for their service.[221] Some, such as Mikhail Zvynchuk, founder of the **Rybar** blog, have also sought to influence foreign audiences, including conducting operations against the US[222] and organising media training courses for Balkan bloggers in Republika Srpska.[223]

Culture and arts actors

Culture and the arts have been used to engage and entertain audiences under the semblance of being apolitical. This grants the Kremlin additional deniability and is crucial for targeting those not predisposed to support Russia's agenda. As with digital media, links to the

216 'Two RT Employees Indicted for Covertly Funding and Directing US Company that Published Thousands of Videos in Furtherance of Russian Interests', US Department of Justice, 4 September, 2024, https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands.

217 Daryna Antoniuk, 'South African InfluencersforHire Target Ukraine's President in Influence Campaign, Researchers Say', The Record,12 May 2025, https://therecord.media/south-african-influencers-anti-zelensky-campaign.

218 Nicolas Quenel, 'AdNow exposed: How Romania became a test lab for Russian interference in the West', Intelligence Online, 3 December 2024, https://www.intelligenceonline.com/government-intelligence/2024/12/03/adnow-exposed-how-romania-became-a-test-lab-for-russian-interference-in-the-west,110347109-evl.

219 Quenel, 'AdNow Exposed'.

220 War correspondents.

221 'Ukraine war: Putin influencers profiting from war propaganda', BBC News, 2 August 2023, https://www.bbc.com/news/world-europe-66653837.

222 Greg Otto, 'State Department offers $10 million reward for info on Russian propaganda outlet', CyberScoop, 21 October 2024, https://cyberscoop.com/rybar-russia-propganda-state-department-reward/.

223 Irvin Pekmez, 'EU Warns Bosnian Serbs over Russian Military Blogger's Planned 'Media School', Balkan Insight, 7 November 2024, https://balkaninsight.com/2024/11/07/eu-warns-bosnian-serbs-over-russian-military-bloggers-planned-media-school/.

CASE STUDY 6: The Social Design Agency

The operations of the SDA are extensive, and the company is likely one of the most significant and highly capable entities in the Kremlin's PDNSA toolkit. To this end, it:

- Operates a vast network of proxy websites that often replicate and imitate legitimate Western sources.
- Produces original content, including news articles and memes.
- Employs influencers and journalists to promote Kremlin narratives worldwide.
- Runs bot farms to propagate its content online.
- Utilises modern technologies, such as AI and deepfakes, to enhance operations.
- Monitors and evaluates the effectiveness of its operations.

Kremlin are indirect and often obscured through various intermediaries such as foundations and NPOs.

Musicians, actors and even poets are frequently employed as propaganda tools by the Kremlin. The late **Iosif Kobzon** served as a key voice in the occupied Donbas region,[224] while patriotic singer **Shaman** has become a symbol of Russia's invasion of Ukraine.[225] This has led some countries, especially the Baltic states, to impose entry bans on Russian musicians, whom they rightly view as the Kremlin's pawns.[226] Moreover, evidence from Moldova's 2024 election interference suggests that Russia is also willing to hire foreign musicians to spread anti-Western messages.[227]

In a sense, every aspect of modern-day Russian culture has become heavily securitised. Russian theatre has come under pressure to promote pro-war messages,[228] and a new military-patriotic theatre is even planned in Moscow.[229] The war has also given rise to a distinctive cultural phenomenon of pro-war poets[230] and a significant increase in pro-war cinema.[231]

Propaganda and disinformation enablers

Various enablers, such as think tanks, PR agencies, NPOs, and IT companies, support the operations of PDNSAs. While not all of them can be classified as PDNSAs themselves, they play a vital role behind the scenes. In most cases, they are financially motivated to work for the regime

224 Tatyana Ovinnikova, 'Pochetnyy grazhdanin Kobzon: kak rossiyskiy pevets stal ruporom Kremlya na Donbasse', Krym.Realii, 8 August 2017, https://ru.krymr.com/a/28663832.html.

225 'Fyuhrer i ego Shaman. Kak Kreml' vossozdayet natsistskuyu estetiku v muzyke dlya propagandy voyny', The Insider, 21 July, 2023, https://theins.ru/obshestvo/263308.

226 'Russian Pop Stars Banned From Entering Latvia Over Ukraine Crisis', The Moscow Times, 21 July 2014, https://www.themoscowtimes.com/archive/russian-pop-stars-banned-from-entering-latvia-over-ukraine-crisis.

227 'Maneliști români, marionetele lui Putin. Cum încearcă să influențeze alegerile din R. Moldova. Jador: Mi s-a propus o sumă mare de bani', Digi24, 31 October 2024, https://www.digi24.ro/stiri/manelisti-romani-marionetele-lui-putin-cum-incearca-sa-influenteze-alegerile-din-r-moldova-jador-mi-s-a-propus-o-suma-mare-de-bani-2989529.

228 'Teatry Rossii na strazhe ideologii: pesy o voyne protiv Ukrainy', Radio Svoboda, 21 October 2023, https://www.svoboda.org/a/teatry-rossii-na-strazhe-ideologii-pjesy-o-voyne-protiv-ukrainy-/32647678.html.

229 Dmitry Novikov, 'Voina prishla v rossiiskie teatry: Kto i kak stavit propagandistskie spektakli ob SVO', Current Time, 18 May 2025, https://www.currenttime.tv/a/voyna-prishla-v-rossiyskie-teatry-kto-i-kak-stavit-propagandistskie-spektakli-ob-svo-/33394369.html.

230 Natalya Granina, 'Tanki idut na zapakh sytykh chuzhikh kvartir', Lenta.ru, 10 June 2023, https://lenta.ru/articles/2023/06/10/zpoets/.

231 Kseniia Shirokova, 'Rossiiskoe kino o voine s Ukrainoi: obrazy, propaganda, umalchivaniia', SOTA Project, 30 June 2024, https://sotaproject.com/article/rossiiskoe-kino-o-voine-s-ukrainoi-obrazy-propaganda-umalchivaniia.

and often maintain informal ties with high-ranking Kremlin figures.

PR agencies have become key enablers of Russia's information confrontation and are directly curated by the Presidential Administration. They frequently collaborate with other private entities, such as IT companies, to build the digital infrastructure required for proxy websites. **The Social Design Agency** (SDA), referred to in leaked documents as Russia's "centre for psychological warfare", is among the most prominent companies serving the Kremlin.[232] It is responsible for several well-documented operations, including **Doppelganger**, **Undercut**, **and Matryoshka**.[233] Along with its affiliated IT company, **Struktura**, it is led by **Ilya Gambashidze**, a political technologist with close ties to the Russian government.[234]

The SDA's operations have proved highly effective in reaching global audiences and convincingly imitating authentic online behaviour and opinion. For instance, content produced by the SDA has reportedly been shared by many authentic Western internet users, including prominent figures such as **Elon Musk** and **Donald Trump Jr**.[235]

IT companies such as **TNSecurity**, **DPKGSoft International**, and **Netshield** play a crucial role in supporting these operations. Some, like **Aeza**, are registered in Russia, while others are based in the West. In some cases, these companies are registered by individuals from post-Soviet countries with no direct connections to Russia, making them difficult to trace and dismantle.[236]

Approximately 15 different NPOs are reportedly involved in orchestrating and funding Russian propaganda since 2022.[237] **Dialog** is the primary NPO involved in orchestrating the activities of the aforementioned PR agencies.[238] Along with the **Expert Institute for Social Research**, Dialog

232 Martin Laine, Anastasia Morozova, 'Leaked files from Putin's troll factory: How Russia Manipulated Western elections', Vsquare, 14 September 2024, https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/.

233 For more detailed information, see public reporting from The Recorded Future and Microsoft.

234 Matthew Kupfer, 'Investigation: Who Is Ilya Gambashidze, the Man the U.S Government Accuses of Running a Kremlin Disinformation Campaign?', Voice of America, 9 May 2024, https://www.voanews.com/a/investigation-who-is-ilya-gambashidze-the-man-the-us-government-accuses-of-running-a-kremlin-disinformation-campaign-/7604052.html.

235 'Fact Check: E! News Did Not Report That USAID Sponsored Celebrity Visits to Ukraine', Reuters, 11 February 2025, https://www.reuters.com/fact-check/e-news-did-not-report-that-usaid-sponsored-celebrity-visits-ukraine-2025-02-11/.

236 Max Bernhard, Alexej Hock, and Sarah Thust, 'Inside Doppelganger – How Russia uses EU companies for its propaganda', CORRECTIV, 22 July 2024, https://correctiv.org/en/fact-checking-en/2024/07/22/inside-doppelganger-how-russia-uses-eu-companies-for-its-propaganda/.

237 'Poznakomtes' s... Da-Da, my nashli eshche odnu propagandistskuyu strukturu Kremlya', Meduza, 26 February 2024, https://meduza.io/feature/2024/02/26/poznakomtes-s-da-da-my-nashli-esche-odnu-propagandistskuyu-strukturu-kremlya.

238 Dialog also produces fakes and orchestrates several high-impact Telegram channels, such as Mash and Readovka. See Mariya Zholobova, Svetlana Reyter, Irina Pankratova i Andrey Pertsev, 'Poznakom'tes' s ANO Dialog. Imenno eta organizatsiya otvechayet zapiar Minoborony RF i sozdaniye feykov pro Ukrainu', Meduza, 18 September 2023, https://meduza.io/feature/2023/09/18/poznakomtes-s-ano-dialog-imenno-eta-organizatsiya-otvechaet-za-piar-minoborony-rf-i-sozdanie-feykov-pro-ukrainu.

develops the ideological frameworks for Putin's regime. Since 2022, both entities have been heavily engaged in Russia's information confrontation with the West. The **Presidential Foundation for Cultural Initiatives** has also been used to fund artists who promote a favourable image of Russia's war in Ukraine.[239]

Think tanks, while categorised primarily as SPNSAs, are also known to act as intermediaries for PDNSAs under the guidance of the RIS. For instance, the Russian **Institute for Strategic Studies** (RISI) has been described by Western analysts as SVR's 'PR arm' and was allegedly involved in interference in the 2016 US presidential election.[240] In turn, the GRU is linked to the Centre for Geopolitical Expertise, led by Kremlin ideologue Aleksandr Dugin, which is used to manage parts of the remnants of the notorious **Internet Research Agency**.[241]

239 'Prezidentskiy fond propagandy', Sirena, 14 September 2022, https://fund-sirena.webflow.io/.

240 Carolina Vendil Pallin and Susanne Oxenstierna, 'Russian Think Tanks and Soft Power', Swedish Defence Research Agency Report (Swedish Defence Agency, August 2017), 30–31, https://www.foi.se/rest-api/report/foi-r--4451--se.

241 Patrick Warren et al., 'Writers of the Storm: Who's Behind the Ongoing Production of Pro-Russian False Narratives', Media Forensics Hub Creative Inquiry Reports (Clemson University, October 2024), 16, https://open.clemson.edu/cgi/viewcontent.cgi?article=1009&context=mfh_ci_reports.

Social and political NSAs

By Andis Kudors and Agata Kleczkowska[242]

Key takeaways

- Russia employs a wide range of social and political non-state actors (SPNSAs) to manipulate, influence, and fragment foreign societies and their decision-making processes.
- Most of these actors project sharp power under the guise of cultural diplomacy and thrive on exploiting democratic values and principles.
- Russia is also using these NSAs to shape legislative processes abroad in ways favourable to the Kremlin.
- Many of these NSAs originate outside Russia, maintaining ambiguous, indirect, or limited ties to the Kremlin, which makes attribution and response by targeted states a highly sensitive and complicated matter.

Introduction

Russia's democratic transition began to slow sharply at the end of Putin's first presidential term and came to a halt during his second. During this period, significant changes were implemented in Russian foreign policy, and the use of SPNSAs expanded in order to pursue two major goals:

- Reducing US influence in international politics, emphasising the need for a multipolar world order; and
- Establishing Russia as one of these poles of global power, positioned to control the former Soviet republics.

To achieve these goals, the Kremlin planned to use soft power instruments, which may be more accurately described as **sharp power:** a set of methods and actors designed to perforate and shatter the information space and political environment of democratic states.[243] The Kremlin sought to build a new normative basis for an international order rooted not in common rules and norms, but in brute force.

A wide variety of SPNSAs have been employed to promote such narratives, both within Russia and abroad, including NGOs, think tanks, compatriots living abroad, and religious organisations. These actors have been used both to advance Russian foreign policy and achieve specific goals, and to weaken democracies in the long term.

Reliance on SPNSAs provides certain advantages compared to state institutions in that they usually have greater public legitimacy and effectiveness.[244] Legitimacy in this context refers to public support for SPNSAs such as NGOs, which are perceived as being free from subordination to a political regime. Effectiveness in the context of SPNSAs refers to the ability of NSAs to adapt swiftly to a new environment and new 'rules of the game', to make quick decisions,

242 This chapter was co-authored by Andis Kudors and Agata Kleczkowska. Andis Kudors provided input for the sections on think tanks, compatriot organisations, sharp power organisations, and history-linked organisations. Agata Kleczkowska authored the sections on political parties and lobbying organisations, while the section on the Russian Orthodox Church was compiled from the inputs of both authors.

243 Christopher Walker and Jessica Ludwig (eds.), 'Sharp Power: Rising Authoritarian Influence', International Forum for Democratic Studies Report (National Endowment for Democracy, December 2017), https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

244 Teresa La Porte, 'The Legitimacy and Effectiveness of Non-State Actors and the Public Diplomacy Concept', *Public Diplomacy Theory and Conceptual Issues*, ISA Annual Convention, San Diego, April 1–4, 2012, 1, https://dadun.unav.edu/server/api/core/bitstreams/217c4a4b-c126–4a95-a43f-3f124861f862/content.

and to influence processes with relatively few resources.

This chapter examines the types of SPNSAs employed by Russia, as well as their operational methods. It also analyses the activities of specific actors supporting the Russian authorities. While this analysis is not intended to be a comprehensive study of the entire field of SPNSAs, it aims to provide insights into the most significant and typical cases in the field, which may arouse readers' interest in conducting further in-depth and expanded research.

Think tanks

The Kremlin has sought ways to challenge the principles of international law and human rights in order to reduce or rebuff criticism of its own domestic disrespect for human rights. Russia has attempted to undermine the notion of the universality of democratic and human rights norms through organisations such as the **Russian Institute for Democracy and Cooperation** (IDC), which was founded in 2007 with this objective in mind.[245]

Several other think tanks have been established for different purposes and audiences. For example, the **Russian International Affairs Council**[246] was set up to engage foreign policy experts and encourage them to support Russia's goals. The council has close ties to the state, as it is chaired by former Minister of Foreign Affairs Igor Ivanov, and Putin's press secretary Dmitry Peskov sits on its presidium.

Another think tank controlled by the Russian government is **RISI**,[247] which until 2009 operated under the SVR.[248] Since then, it has been formally subordinated to the Kremlin and consistently headed by former high-ranking SVR officers, including Mikhail Fradkov and Leonid Reshetnikov.[249]

Additionally, **the Institute for CIS Countries, Diaspora and Integration** (CIS Institute) was established in 1996 but expanded its activities under Putin, with the aim of conducting research on sociopolitical processes in the 'near abroad' and providing legal, political and cultural support for compatriots living abroad.[250] The CIS Institute is headed by State Duma member Konstantin Zatulin. According to the Estonian Foreign Intelligence Service (EFIS), the CIS Institute has long been closely associated with the FSB, specifically the 5th Service,[251] which

245 Russian Foreign Minister Sergei Lavrov noted that the Paris and New York branches of the IDC have become an important platform for Russian politicians and public figures. See 'Institute of Democracy and Cooperation Opens in Paris', GMF, https://securingdemocracy.gmfus.org/incident/institute-of-democracy-and-cooperation-opens-in-paris/; 'Summary of Remarks by Minister of Foreign Affairs Sergey Lavrov at a Meeting with Representatives of Russian Nongovernmental Organizations, Moscow', Ministry of Foreign Affairs, 18 February 2010, https://www.mid.ru/en/foreign_policy/news/1637043/.

246 'General Information', Russian International Affairs Council, 18 April 2025, https://russiancouncil.ru/en/about/.

247 The Russian Institute for Strategic Studies (RISI) is also covered in the chapter on PDNSAs.

248 'International Security and Estonia 2023', Estonian Foreign Intelligence Service Report, (EFIS, 8 February 2023), https://raport.valisluureamet.ee/2023/en/.

249 'Rukovodstvo. Reshetnikov Leonid Petrovich', RISS, https://web.archive.org/web/20140331072409/https://www.riss.ru/index.php/jomsocial/profile/613-reshetnikov-leonid-petrovich/.

250 'Institut stran SNG', ISNG, https://i-sng.ru/institut-stran-sng/.

251 'International Security and Estonia 2023', EFIS.

played an important role in advising Russian foreign policy decision-makers before Russia's full-scale invasion of Ukraine.

Compatriot organisations

Numerous NGOs are involved in implementing Russia's policy towards Russians living abroad, whose hearts and minds Moscow seeks to win. These organisations focus on three main areas:

- The protection of human rights;
- The popularisation of the Russian language, culture and Orthodoxy;
- The falsification of the history of Russia and its neighbouring countries.

One of the most important entities dealing with compatriot issues abroad is the **Foundation for the Support and Protection of the Rights of Compatriots Living Abroad** (Pravfond), established in 2012.[252] Its stated mission is to defend Russian compatriot activists by providing legal assistance. Since its establishment, the foundation has financed the activities of Kremlin influence agents and paid for lawyers when legal problems arise. Several of these individuals are currently on trial for aiding Russia and inciting hatred.[253] The person responsible for the Baltic states at Pravfond, **Vladimir Pozdorovkin**, was identified by the Estonian Internal Security Service (KAPO) as an SVR officer.[254]

Pravfond has been particularly active in countries with large Russian populations, such as Latvia, where the largest recipients of funds were the **Legal Protection Centre** (TAC)[255] and the **Latvian Human Rights Committee** (LCK).[256] Both TAC and LCK reportedly received a total of 718,000 euros over a ten-year period to cover the legal expenses of Russian influence agents.[257]

Pravfond also provided financial assistance to the **European Russian Alliance** (ERA), created by LCK's leader **Tatjana Ždanoka** and registered in France in 2014.[258] ERA's stated goal was to support Russia's foreign policy objectives within the EU.

Sharp power organisations

Sharp power organisations differ from compatriot organisations in that they seek to influence a much broader global audience through cultural diplomacy, although their activities may overlap.

In Russia's case, cultural diplomacy frequently functions as an instrument of sharp power and hybrid threats, emanating from several organisations closely aligned with the state. One such entity promoting Russian culture and language abroad is the **Russkiy Mir Foundation** (RMF), established in 2007. The foundation's name draws on the concept of the so-called "Russian world" (*Russkiy mir*), which envisions the unification of Russians

252 'Fond podderzki i zashchiti prav sootechestvennikov prozhivaiushchih za rubezhom', Pravfond, https://pravfond.ru/.
253 Inga Spriņģe, 'Uzmanību! Uzmanību! Runā Kremlis!', Re:Baltica, 3 June 2024, https://rebaltica.lv/2024/06/uzmanibu-uzmanibu-runa-kremlis/.
254 'Annual Review 2007', Kaitsepolitseiame Report (KAPO, 2007), https://kapo.ee/en/content/annual-reviews/.
255 Tiesiskās aizsardzības centrs (TAC).
256 Latvijas cilvēktiesību komiteja (LCK).
257 Inga Spriņģe, 'Uzmanību! Uzmanību! Runā Kremlis!'
258 Ibid.

CASE STUDY 7: Falsification of history in the Baltic states

Russian NGOs promote 9 May as Victory Day in the Baltic states, ignoring the fact that Latvians, Estonians and Lithuanians celebrate the end of World War II on 8 May alongside the rest of Europe, while 9 May is associated with the second Soviet occupation. Russian historical propagandists exacerbate the cultural trauma experienced by the Baltics that resulted from the Soviet occupation, when tens of thousands of Latvians, Lithuanians and Estonians were deported to Siberia because of their ethnic and social origin.

This messaging is often channelled through local organisations. One such NGO in Latvia is the 9 May Organisation, which has received financial support from Russia and has pledged to play an active role in organising the Victory Day celebrations in Riga and distributing St George's ribbons in Russian minority schools. The ribbons have become a symbol of Russia's occupation of Crimea and its aggression against Ukraine.

and Russian-speaking non-Russians in a cross-border formation. Vyacheslav Nikonov,[259] a political scientist with close ties to the Russian government, was appointed executive director of the foundation. The RMF actively cooperates with and distributes financial support to various NGOs, particularly in countries with a large proportion of Russian speakers, with the aim of promoting the Russian language and Russia's historical interpretation.

Another important entity is the **Alexander Gorchakov Public Diplomacy Foundation**,[260] established in 2010. It is chaired by Foreign Minister Sergei Lavrov, and its board of directors includes the US-sanctioned oligarch Alisher Usmanov and the head of the Rossotrudnichestvo agency, Yevgeny Primakov Jr.[261] In 2022, the EU imposed sanctions on the foundation, stating that it actively supports the Russian government responsible for the annexation of Crimea and the destabilisation of Ukraine.[262] Ukraine had already closed the foundation's office in Kyiv in 2015 for spreading anti-government propaganda.

History-linked organisations

During Putin's time in office, history has become increasingly politicised. In order to instrumentalise interpretations of the past that serve the goals of the Russian leadership, the **Historical Memory Foundation** (HMF) was founded in 2008. The HMF organises events such as discussions, conferences, and seminars, and publishes books and journals on various historical topics.[263] Its director, **Alexander Dyukov**,[264] who has been declared persona non grata by Latvia, is known for "cherry picking" documents from the FSB's Central Archive to produce HMF publications. This practice illustrates the FSB's interest in promulgating a biased interpretation of history to achieve the Kremlin's goals.

Estonia in particular has suffered from destructive activities in the sphere of history politics. For instance, pro-Russian organisation **Night Watch**, established in 2007, played a central role in the violent protests against Tallinn's decision to relocate a monument dedicated to Soviet soldiers who fell in World

259 Nikonov is a member of the State Duma and a grandson of the Soviet Minister of Foreign Affairs, Vyacheslav Molotov.

260 The Foundation is named after Alexander Gorchakov, who was Tsarist Russia's Minister of Foreign Affairs from 1856 to 1882.

261 Primakov Jr. is the grandson of former Russian Minister of Foreign Affairs and Prime Minister Yevgeny Primakov.

262 'European Union's Sanction Packages Against Russia: Contents and Implications', *Eurasian Research Journal* (ERJ), Vol. 5, No. 3 (Summer 2023): 90, https://dergipark.org.tr/en/download/article-file/3378350.

263 Ainārs Lerhis, 'Vēstures jautājumi Krievijas publiskajā diplomātijā', in *Krievijas publiskā diplomātija Latvijā: mediji un nevalstiskais sektors*, ed. Andis Kudors (Rīga: APPC, LU Apgāds, 2014), 177.

264 Dyukov has collaborated with another imperial-minded Russian historian and political scientist, president of the Historical Perspectives Foundation Natalya Narochnitskaya.

CASE STUDY 8: The role of the Russian Orthodoxy in justifying military aggression against Ukraine

Two weeks before the annexation of Crimea, Vsevolod Chaplin, head of the Synodal Department for Church and Public Relations of the Moscow Patriarchate, issued a statement indicating that the ROC had called on the Ukrainian side not to resist Russian military operations in Ukraine. This stance aligned with the primary task of Russia's information confrontation: compelling the Kremlin's adversaries to surrender. Moreover, it directly corresponded to the goals of official Russia in the occupation and subsequent annexation of Crimea. According to Moscow's plan, the process was to unfold swiftly, with minimal casualties among Russian soldiers and little or no resistance from the Ukrainian side.

War II[265] from the city centre to the Defence Forces Cemetery. During these riots, police detained around 1,200 people, another 50 were injured, and one person was killed.[266] KAPO later reported that Russian-speaking extremist groups in Estonia, including Night Watch, sought to incite national hatred by exploiting differing interpretations of history.[267]

The Russian Orthodox Church (ROC)

Religious organisations provide states with a platform to reach segments of society in target countries that secular actors are unable to reach. The ROC has been participating in Russia's public diplomacy since 2003, when it concluded a cooperation agreement with the Ministry of Foreign Affairs (MFA).[268]

Orthodoxy is heavily securitised in Russia, meaning that military and security institutions pay particular attention to the Moscow Patriarchate. The ROC has signed cooperation agreements with several state institutions,[269] and Orthodox chapels have been installed in the Moscow office of the FSB as well as in Russian diplomatic missions abroad.[270] Alignment between the ROC and the security apparatus can be seen in **Case Study 8**.[271]

After the full-scale invasion of Ukraine, the Moscow Patriarchate became even more openly supportive of Russia's aggression and promoted the sacralisation of the war. The idea of a *holy war*, formulated by the **World Russian People's Council** under **Patriarch Kirill**,[272] contributed to the demonisation of the enemy and the escalation of hostilities.

There is also evidence that Russia uses the ROC to influence socio-political processes in other Orthodox states. One example is the **Serbian Orthodox Church** (SOC), with around eight million members.[273] As concluded by Professor Vesko Garčević, it is not only "more influential and powerful than any individual political figure",[274] but also serves as "an important node in a network spanning politics,

265 The so-called Bronze Soldier or *Alyosha*.

266 'Savisārs: nekārtības Rīgā un Tallinas nemieri nav salīdzināmi', DELFI, 15 January 2009, http://www.delfi.lv/news/world/baltics/savisars-nekartibas-riga-un-tallinas-nemieri.d?id=22937554.

267 'Annual Review 2008', Kaitsepolitseiame Report (KAPO, 2008): 26, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202008.pdf.

268 Robert C. Blitt, 'Russia's Orthodox Foreign Policy: The Growing Influence of the Russian Orthodox Church in Shaping Russia's Policies Abroad', *University of Pennsylvania Journal of International Law*, Vol. 33, No. 2, (2011), https://ssrn.com/abstract=1725522 or http://dx.doi.org/10.2139/ssrn.1725522.

269 Such as the Ministry of Education, the Ministry of Health, the Ministry of Internal Affairs and the Ministry of Defence.

270 'Annual Review 2008', KAPO.

271 The case study was provided by Andis Kudors.

272 'Nakaz XXV Vsemirnogo russkogo narodnogo sobora 'Nastoyashcheye i budushcheye Russkogo mira'', Patriarhia, 27 March 2024, https://www.patriarchia.ru/db/text/6116189.html.

273 Elizabeth Mohn, 'Serbian Orthodox Church', EBSCO Research Starters, 2025, https://www.ebsco.com/research-starters/history/serbian-orthodox-church.

274 Vesko Garčević, 'The Serbian Orthodox Church and Extreme-Right Groups: A Marriage of Convenience or Organic Partnership?', Berkley Forum, 14 July 2023, https://berkleycenter.georgetown.edu/posts/the-serbian-orthodox-church-and-extreme-right-groups-a-marriage-of-convenience-or-organic-partnership.

traditional and social media, and academia" across Serbian communities.[275] The SOC provides religious legitimacy to domestic and foreign state policies in Serbia, promotes Serbian nationalism, and supports nationalist and far-right groups and individuals who often advocate closer ties with Russia.[276]

The SOC is "both a channel for Russian narratives, a tool employed by Russia to sow divisions, and a political actor in itself that supports pro-Russian politicians and Serb nationalism".[277] Although it is not subordinate to the Moscow Patriarchate, clear links exist between the two organisations. One tangible example of this is Russia's financial contribution to the construction of Belgrade's St Sava Cathedral. Of the estimated €100 million cost, €10 million allegedly came from Russia, including from the state-owned **Gazprom**.[278]

The SOC is also highly influential and trusted in Montenegro. In fact, there are two competing Orthodox factions in the state: the **Metropolitanate of Montenegro and the Littoral** (which is part of the SOC) and the **Montenegrin Orthodox Church** (which is canonically unrecognised and has operated as an NGO).[279] In December 2019, Montenegro's parliament adopted the Law on Freedom of Religion, which demanded "broader state insight into the finances of religious communities".[280] The most controversial provisions concerned "the nationalisation of church property if the SOC cannot provide proof of ownership before 1918, when Montenegro became an integral part of the Kingdom of Serbs, Croats, and Slovenes".[281] The law drew criticism from the Russian government, the ROC, the Night Wolves,[282] and the SOC, among others, reflecting the interlinked nature of these actors.

Political parties

Russia has cultivated relationships with certain political parties, parliamentarians and individual politicians in other countries. However, in the overwhelming majority of cases, descriptions of these links are based solely on media reports and lack confirmation from official sources.

Through such intermediaries, Russia gains the opportunity to influence national and EU legislation in line with its interests. Politicians associated with Russia, such as the aforementioned **Tatjana Ždanoka**, have voted against resolutions condemning Russia

275 Ibid.
276 Wouter Zweers, Niels Drost, and Baptiste Henry, 'Little Substance, Considerable Impact: Russian Influence in Serbia, Bosnia and Herzegovina, and Montenegro', Clingendael Report (Clingendael, August 2023), 21–22, https://www.clingendael.org/sites/default/files/2023-08/little-substance-considerable-impact.pdf.
277 Ibid., 22.
278 Mladen Aleksic, 'More Than a Church – New 'Hagia Sophia' is Big Deal for Serbia', Balkan Insight, 23 October 2020, https://balkaninsight.com/2020/10/23/more-than-a-church-new-hagia-sophia-is-big-deal-for-serbia/.
279 Mira Milosevich, 'Russia's Weaponization of Tradition: The Case of the Orthodox Church in Montenegro', CSIS, 25 September 2020, https://www.csis.org/blogs/post-soviet-post/russias-weaponization-tradition-case-orthodox-church-montenegro.
280 Ibid.
281 Ibid.
282 Ibid.

or supporting Ukraine in legislative bodies.[283] The same politicians have served as observers during elections held in Russia and Crimea.[284] Additionally, some political parties and their leaders have reportedly endorsed the conclusion of favourable investment treaties between their governments and Russia, including in the energy sector,[285] as well as other cooperation agreements related to security and joint military exercises.[286] In general, these actors often promote anti-Western, anti-EU, and anti-NATO rhetoric consistent with the Kremlin's agenda,[287] or call for closer alliances between their respective states and Russia.[288]

Links between political parties and Russia vary significantly (see **Table 5**). On the one hand, some parties are allegedly financed by Russia,[289] or Russia has reportedly invested in the regions where these parties operate[290] through complicated schemes and offshore entities registered to Russian citizens with no apparent connection to the Kremlin.[291]

283 'Latvian MEP refuses to condemn Russian invasion of Ukraine', LSM+, 2 March 2022, https://eng.lsm.lv/article/politics/politics/latvian-mep-refuses-to-condemn-russian-invasion-of-ukraine.a445994/; Romain Lemaresquier, 'France: un gouvernement d'extrême droite "serait une catastrophe en matière de politique étrangère"', RFI, 14 June 2024, https://www.rfi.fr/fr/europe/20240614-france-un-gouvernement-d-extr%C3%AAme-droite-serait-une-catastrophe-en-mati%C3%A8re-de-politique-%C3%A9trang%C3%A8re; see also 'Nationalists vow to topple Bulgarian cabinet over Russia', Euractiv, 2 April 2014, https://www.euractiv.com/section/global-europe/news/nationalists-vow-to-topple-bulgarian-cabinet-over-russia/.

284 Sanita Jemberga et al., 'Kremlin's Millions', Re:Baltica, 27 August 2015, https://en.rebaltica.lv/2015/08/kremlins-millions/.

285 Maksim Samorukov, 'Surviving the War: Russia-Western Balkan Ties After the Invasion of Ukraine', Carnegie Endowment for International Peace, 25 April 2023, https://carnegieendowment.org/russia-eurasia/politika/2023/04/surviving-the-war-russia-western-balkan-ties-after-the-invasion-of-ukraine?lang=en.

286 Predrag Petrović, 'Serbia: Government and the Scarecrow', in *Russia and the Far-Right. Insights from Ten European Countries*, eds. Kacper Rekawek, Thomas Renard and Bàrbara Molas (The Hague: International Centre for Counterterrorism, 2024), 84–86.

287 Wouter Zweers, Niels Drost and Baptiste Henry, 'Little substance, considerable impact'; 'Investigation alleges Russian money behind political party in neighboring Georgia', GMF Alliance for Securing Democracy, https://securingdemocracy.gmfus.org/incident/investigation-alleges-russian-money-behind-political-party-in-neighboring-georgia/; Péter Krekó, 'I am Eurasian – The Kremlin connections of the Hungarian far-right', Heinrich-Böll-Stiftung European Union, 5 May 2015, https://eu.boell.org/en/2015/05/05/i-am-eurasian-kremlin-connections-hungarian-far-right.

288 Shaun Walker, ''It's not about what is fair': Macedonians prepare to vote on name change', The Guardian, 10 September 2018, https://www.theguardian.com/world/2018/sep/10/its-not-about-what-is-fair-macedonians-prepare-to-vote-on-name-change.

289 See Matea Jerković, 'Russia Needs the Unstable Balkans', in *A Year Later: War in Ukraine and Western Balkan (Geo)Politics*, eds. Jelena Džankić, Simonida Kacarska and Soeren Keil (San Domenico di Fiesole: European University Institute, 2023), 98, 103; Mariam Kiparoidze and Katia Patin, 'Investigation alleges Russian money behind political party in neighboring Georgia'; 'How the Kremlin interferes in the domestic politics of neighboring countries. Part One: Elections in Georgia', Dossier Center, 24 August 2020, https://dossier.center/georgia/?fbclid=IwAR1Tt2SVkHtaVWRLUoVDlwUJ40HzfgIOQnl35J_4AzaK9qvADCs7SVV5gI0.

290 Jerković, 'Russia Needs the Unstable Balkans', 103.

291 Danijel Kovacevic, 'Bosnian Serb Parties Battle Over Mysterious Loan', Balkan Insight, 27 November 2015, https://balkaninsight.com/2015/11/27/bosnian-serb-government-and-opposition-fight-over-suspicious-

CASE STUDY 9: Western politicians and Russian intelligence

In 2022, the Hungarian Supreme Judicial Council found Béla Kovács "guilty of the crimes of espionage and budget fraud against the institutions of the EU and of the misdemeanour of falsifying private documents", sentencing him to five years in prison and a ten-year ban from public affairs (Baranya 2022). According to the Mandiner portal, the accusation centred on claims that, between 2012 and 2014, Kovács "provided information to Russian intelligence agencies on, among other things, energy matters, the European Parliament elections, the domestic political situation in Hungary, and the expansion of the Paks nuclear power plant" (Baranya 2022; *Hungary Today* 2022).

In the case of Tatjana Ždanoka, the Latvian State Security Service initiated criminal proceedings against her on suspicion of her "possible cooperation with Russia's intelligence and security services". Investigative journalists have claimed to possess definitive proof of Ždanoka's collaboration with the FSB (State Security Service 2024).

Media sources have also claimed that certain party members have received donations from Russian oligarchs or other individuals linked to the Kremlin.[292] Moreover, some political parties are alleged to have been "guided" and "supervised" by companies affiliated with the Russian government,[293] while their members are said to have undergone training conducted by figures connected to the Kremlin.[294] There are also accounts of meetings between certain politicians and high-ranking Russian officials, as well as visits to Moscow.[295] Some party leaders have even been awarded prestigious Russian medals.[296] Finally, there are several cases of cooperation agreements signed between political parties and Putin's *United Russia*.[297] In recent years, however, a number of parties, including **Estonia's Centre Party**, **Latvia's Harmony**, and **Italy's Lega**, declared that such agreements were no longer valid or enforced.[298]

loan-11–27–2015/; Suzanne Daley and Maïa de la Baume, 'French Far Right Gets Helping Hand With Russian Loan', The New York Times, 1 December 2014, https://www.nytimes.com/2014/12/02/world/europe/french-far-right-gets-helping-hand-with-russian-loan-.html.

292 James Oliver, Steve Swann and Nassos Stylianou, 'Tory donor's "link" to sanctioned oligarch's secret London property', BBC, 21 April 2022, https://www.bbc.com/news/uk-politics-61080537; Catherine Belton, 'In British PM race, a former Russian tycoon quietly wields influence', Reuters, 19 July 2019, https://www.reuters.com/investigates/special-report/britain-eu-johnson-russian/.

293 'Investigation alleges Russian money behind political party in neighboring Georgia'.

294 'Updated: Largest Opposition Party in Macedonia is Not Boycotting Name Referendum', VOA, 17 September 2018, https://www.voanews.com/a/fact-check-macedonia-name-change-boycott/6741927.html.

295 Arlinda Rrustemi et al., eds., 'Geopolitical Influences of External Powers in the Western Balkans', HCSS Security Report, (Hague Centre for Strategic Studies, September 2019), 116, https://hcss.nl/wp-content/uploads/2021/01/Geopolitical-Influences-of-External-Powers-in-the-Western-Balkans0.pdf; Wouter Zweers, Niels Drost and Baptiste Henry, 'Little substance, considerable impact', 19; Lemaresquier, 'France: un gouvernement d'extrême droite 'serait une catastrophe en matière de politique étrangère'', RFI, 14 June 2024, https://www.rfi.fr/fr/europe/20240614-france-un-gouvernement-d-extr%C3%AAme-droite-serait-une-catastrophe-en-mati%C3%A8re-de-politique-%C3%A9trang%C3%A8re; Sarah Elzas, 'Has France's far-right National Rally turned on Russia?', RFI, 26 June 2024, https://www.rfi.fr/en/france/20240626-has-france-s-far-right-national-rally-really-turned-on-russia.

296 Petrović, 'Serbia: Government and the Scarecrow', 84; Jo Simmons, 'The Curious Tale of Bulgaria's Extremist Flip-Flopping Party', The Huffington Post, 3 June 2014, https://www.huffingtonpost.co.uk/jo-simmons/volen-siderov-ataka_b_5432359.html.

297 See Zweers, Drost and Henry, 'Little substance, considerable impact', 19; Petrović, 'Serbia: Government and the Scarecrow', 77, 84.

298 'Ratas: Center Party not planning to give up protocol with United Russia', ERR, 9 October 2017, https://news.err.ee/635273/ratas-center-party-not-planning-to-give-up-protocol-with-united-russia; 'Center Party board annuls agreement with United Russia', ERR, 6 March, 2022, https://news.err.ee/1608522557/center-party-board-annuls-agreement-with-united-russia; 'Italy's League disavows accord with Russia's ruling party', *Reuters*, 2 April 2024, https://www.reuters.com/world/europe/italys-league-disavows-accord-with-russias-ruling-party-2024–04–02/.

TABLE 5. Forms of cooperation between foreign political parties and Russia

Official cooperation	**Unofficial cooperation**	**Strategically aligned**
Political parties that have signed official cooperation agreements with United Russia or other "systemic" political parties in Russia.	Political parties reliant on Russian investments or covert financing, sometimes working for the RIS.	Political parties pursuing their own political agendas but using favourable financial and political relations with Russia as leverage.
Example: Social Democratic Party Harmony (Latvia)	**Example:** Often the most difficult to verify, as confirmation typically requires a court ruling.	**Example:** Serbian Progressive Party (Serbia)

The cases of **Béla Kovács**, former member of Hungary's **Jobbik party**, and **Tatjana Ždanoka**, former leader of the **Latvian Russian Union**, are somewhat different and exemplify how Western politicians may be exploited more directly by the RIS (see **Case Study 9**).[299]

Lobbyist organisations

This category includes various organisations that, despite their stated aims, work to persuade foreign states to influence legal processes or political discourse in line with Russian policies and rhetoric. A pivotal example is the **Human Rights Accountability Global Initiative Foundation** (HRAGIF), officially described as "an institution dedicated to making it possible for American families to adopt Russian children".[300] It was founded by the owner of a real estate investment company[301] connected through family ties to the Russian government.[302] The company was reportedly involved in a tax fraud[303] uncovered by Sergei Magnitsky, a Russian tax lawyer and auditor.[304] Magnitsky's subsequent death in

299 In the case of Tatjana Ždanoka, the Latvian State Security Service initiated criminal proceedings against her on suspicion of her "possible cooperation with Russia's intelligence and security services" (State Security Service 2024). Investigative journalists have claimed to possess definitive proof of Ždanoka's collaboration with the FSB (Latvijas Sabiedriskais Medijs 2024); Róbert Baranya, 'Öt év fegyházbüntetésre ítélte kémkedés miatt a Kúria a volt jobbikos Kovács Bélát', Mandiner, 27 September 2022, https://mandiner.hu/belfold/2022/09/kovacs-bela-jobbik-itelet-kuria-kemkedes; 'Former Jobbik MEP Sentenced for Espionage for Russia', Hungary Today, 28 September 2022, https://hungarytoday.hu/former-jobbik-mep-sentenced-for-espionage-for-russia/; 'VDD carries out criminal proceedings in the criminal case against Tatjana Ždanoka', State Security Service, 24 July 2024, https://vdd.gov.lv/en/news/press-releases/vdd-carries-out-criminal-proceedings-in-the-criminal-case-against-tatjana-zdanoka; 'Latvian MEP Zdanoka Named as Russian FSB Asset', Latvijas Sabiedriskais Medijs, 29 January 2024, https://eng.lsm.lv/article/politics/politics/29.01.2024-latvian-mep-zdanoka-named-as-russian-fsb-asset.a540771/.

300 Jackie Northam, 'Behind Support For "Adoption," A Web Of Clandestine Russian Advocates', NPR, 7 September 2017, https://www.npr.org/2017/09/07/548886521/behind-support-for-adoption-a-web-of-clandestine-russian-advocates.

301 Paul Radu and Olesya Shmagun, 'Prevezon Holdings: The Black Money Collector', OCCRP, 17 November 2020, https://www.occrp.org/en/project/the-fincen-files/prevezon-holdings-the-black-money-collector; Brendan Pierson, 'US judge orders Russian-owned company to pay $6 million settlement', *Reuters*, 2 February 2018, https://www.reuters.com/article/business/us-judge-orders-russian-owned-company-to-pay-6-million-settlement-idUSKBN1FM2R3/.

302 Michael Weiss, 'Russian firm that promised to pay US millions after money-laundering settlement misses deadline', CNN, 2 November 2017, https://edition.cnn.com/2017/11/02/world/russia-money-laundering-deadline-missed/index.html.

303 Radu and Shmagun, 'Prevezon Holdings'.

304 Sergei Magnitsky was a lawyer who uncovered large-scale tax fraud by Russian officials. Arrested in 2008, he died in custody after torture and neglect. In response, financier and activist Bill Browder led the campaign that resulted in the US Sergei Magnitsky Rule of Law Accountability Act (2012), which authorised sanctions

a Russian prison led to the adoption of the Sergei Magnitsky Rule of Law Accountability Act of 2012, followed by the Global Magnitsky Human Rights Accountability Act passed by the US Congress in 2016.[305] The HRAGIF allegedly campaigned to persuade members of Congress to oppose the bill or at least remove Magnitsky's name from its title.[306] Despite these efforts, the Global Magnitsky Human Rights Accountability Act was successfully adopted in the US and later became a model for similar legislation worldwide.[307]

Another example is the Canadian Justice for Victims of Corrupt Foreign Officials Act, adopted in October 2017. According to Dan Levin and Jo Becker of *The New York Times*, when Canadian lawmakers were still working on the Act, the **Russian Congress of Canada** (RCC) attempted to obstruct their efforts.[308] Canadian Member of Parliament John McKay stated that the RCC coordinated its lobbying activities against the legislation with the Russian Embassy in Ottawa.[309] The RCC allegedly "sent letters to members of parliament calling for Canada to withdraw its support for the Magnitsky legislation".[310] As in the US case, however, the organisation's efforts were ultimately unsuccessful.

An additional example is the **International Agency for Current Policy** (IACP), which vaguely described itself as a "closed association of professionals" that aimed to "cooperate with leading EU parliamentary parties and individual politicians".[311] According to Tatiana Tkachenko

against those responsible for his death and other perpetrators of torture, extrajudicial killings, and gross human rights abuses. See 'Russia uses a US non-profit to hide funding of covert lobbying operation against Russia sanctions', GMF Alliance for Securing Democracy, https://securingdemocracy.gmfus.org/incident/russia-uses-a-u-s-non-profit-to-hide-funding-of-covert-lobbying-operation-against-russia-sanctions/; Luke Harding, 'Who was Sergei Magnitsky and how did UK sanctions come about?', The Guardian, 6 July 2020, https://www.theguardian.com/politics/2020/jul/06/who-was-sergei-magnitsky-and-how-did-uk-sanctions-come-about; 'Sergei Magnitsky Rule of Law Accountability Act of 2011', US Congress, https://www.congress.gov/congressional-report/112th-congress/senate-report/191/1; Michael A. Weber, 'Human Rights and Anti-Corruption Sanctions: The Global Magnitsky Human Rights Accountability Act', Congressional Research Service, 7 November 2024, https://www.congress.gov/crs-product/IF10576.

305 The latter allowed the US president to "impose sanctions with respect to foreign persons responsible for gross violations of internationally recognised human rights" anywhere in the world. See Section 3, Global Magnitsky Human Rights Accountability Act, 114th Congress (2015–2016), S.284.

306 Jessikka Aro, *Trolle Putina* (Kraków: SQN, 2020), 138–141.

307 See Martin Russell, 'Global human rights sanctions – Mapping Magnitsky laws: The US, Canadian, UK and EU approach', European Parliamentary Research Service Briefing (European Parliament, November 2021), https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698791.

308 Dan Levin and Jo Becker, 'Canadian Lawmakers Say Pro-Russia Group Tried to Derail Sanctions Law', The New York Times, 4 October 2017, https://www.nytimes.com/2017/10/04/world/canada/russia-magnitsky.html#).

309 Ibid.

310 In the letters, the RCC reportedly claimed that the bill would harm Canada's interests, accused its supporters of anti-Russian bias, and "suggested that deaths in Canadian prisons could be used as a basis for sanctions against Canadian officials by other governments". See Levin and Becker, 'Canadian Lawmakers'.

311 Martin Laine et al., 'Kremlin-Linked Group Arranged Payments to European Politicians to Support Russia's Annexation of Crimea', OCCRP, 3 February 2023, https://www.occrp.org/en/investigation/kremlin-linked-group-arranged-payments-to-european-politicians-to-support-russias-annexation-of-crimea.

and Martin Laine, the IACP lobbied European politicians to promote "pro-Russian motions (...) largely focused on legitimising Russia's annexation of Crimea".[312] Allegedly, its leadership maintained close ties with senior Russian politicians, including one of Putin's key advisers at the time.[313]

In 2016, the IACP collaborated with a member of the Veneto regional parliament, which became the first region in an EU member state to adopt a resolution on lifting sanctions against Russia.[314] In the same resolution, Veneto also urged Italy's national government to abandon the EU's common foreign policy and recognise Crimea as Russian territory.[315] Regional parliaments in Liguria and Lombardy followed Veneto's example, passing their own resolutions "recognising" Crimea as part of Russia.[316]

The IACP was also active in Cyprus. According to investigative journalists, in 2016 the Agency began working on a resolution "On lifting sectoral economic sanctions against Russia", intended for adoption by the House of Representatives of the Cypriot Parliament. The IACP's associates exchanged correspondence, including a draft text, and the Cypriot Parliament subsequently adopted a nearly identical document. The resolution called on the government "to work towards lifting EU sanctions imposed on Russia over its involvement in the Ukraine conflict"[317] and stated that the EU sanctions on Russia had proved "counterproductive and in no way helped to resolve the crisis in Ukraine".[318] According to the journalists' investigation, "[t]he documents also detail separate projects for Latvia, Greece, and even the Parliamentary Assembly of the Council of Europe".[319]

Reportedly, the IACP also organised visits to Crimea for various European politicians. For instance, nine politicians from Austria, Germany, Italy, the Czech Republic, and Poland allegedly attended the Yalta International Economic Forum and received honoraria for their participation in the event.[320] The organisation also helped arrange visits by European observers to elections held in Russia and Crimea. Among them were politicians from the Czech Republic, Slovakia, the Netherlands, Belgium, France, Sweden, and Italy.[321]

312 Tatiana Tkachenko and Martin Laine, 'How a Russian Influence Group Infiltrated Cypriot Party Politics', OCCRP, 3 February 2023, https://www.occrp.org/en/investigation/how-a-russian-influence-group-infiltrated-cypriot-party-politics.
313 Laine et al., 'Kremlin-Linked Group Arranged Payments'.
314 'Kremlin-linked lobbyists paid European politicians to legitimise annexation of Crimea', Ukrainska Pravda, 3 February 2023, https://www.pravda.com.ua/eng/news/2023/02/3/7387835/.
315 'Italian region votes to scrap anti-Russian sanctions', Euronews, 18 May 2016, https://www.euronews.com/2016/05/18/italian-region-votes-to-scrap-anti-russian-sanctions.
316 'Kremlin-linked lobbyists paid European politicians.'
317 'Cyprus parliament calls for end to EU sanctions on Russia', Euractiv, 8 July 2016, https://www.euractiv.com/section/global-europe/news/cyprus-parliament-calls-for-end-to-eu-sanctions-on-russia/.
318 Ibid.
319 'Kremlin-linked lobbyists paid European politicians.
320 Ibid.
321 Ibid.

Another example is **Voice of Europe**, officially a media portal with roots in the Netherlands,[322] created and funded by a Ukrainian oligarch allegedly closely linked to Putin.[323] The outlet's YouTube channel became a platform for some EU lawmakers, including members of far-right parties, to criticise EU policies. There is no suggestion that those appearing on the channel accepted payment.[324] However, according to media reports confirmed by Polish, Czech and Belgian security services, as well as by the prime ministers of Belgium and Czechia, "certain MEPs and candidates in the upcoming European elections [in 2024] have received payment from the Russian government or its proxies to spread propaganda and disinformation and to influence the elections to the European Parliament in various European countries".[325] Voice of Europe was allegedly involved in these influence operations.[326]

322 Nicholas Vinocur, Pieter Haeck and Eddy Wax, 'Russian influence scandal rocks EU', Politico, 29 March 2024, https://www.politico.eu/article/voice-of-europe-russia-influence-scandal-election/.

323 Filip Bryjka, 'Unravelling Russia's Network of Influence Agents in Europe', PISM, 5 April 2024, https://pism.pl/publications/unravelling-russias-network-of-influence-agents-in-europe; Etienne Bouche, 'Another Ukraine: a disinformation platform run by an exiled Ukrainian oligarch in Russia', France 24, 29 February 2024, https://www.france24.com/en/europe/20240229-other-ukraine-disinformation-platform-run-exiled-ukrainian-oligarch-russia.

324 Vinocur, Haeck and Wax, 'Russian influence scandal rocks EU'.

325 'European Parliament resolution of 25 April 2024 on new allegations of Russian interference in the European Parliament, in the upcoming EU elections and the impact on the European Union', 2024/2696(RSP), para. F.

326 Ibid, para. G, I, O, 2, 10, 29; Vinocur, Haeck and Wax, 'Russian influence scandal rocks EU'.

Economic and financial NSAs

By Eliza Lockhart

Key takeaways

- The Russian state leverages a network of economic and financial non-state actors (EFNSAs) to generate revenue, maintain economic resilience under sanctions, and wield financial and political influence abroad.
- As Western sanctions have intensified, EFNSAs have been increasingly mobilised to absorb domestic fiscal shocks and support the Kremlin's broader strategic posture.
- They are often owned and controlled by Russian oligarchs who serve as investors, facilitators and intermediaries for state-sanctioned activities in return for access to state contracts and protection.
- They often act as extensions of state policy, although the exact level of control exercised by the Kremlin can be challenging to determine.

Introduction

Russia's full-scale invasion of Ukraine in 2022 marked a dramatic escalation in its confrontation with the West – not only on the battlefield, but also across the economic and financial domains. In response to unprecedented sanctions, Russia mobilised a diverse ecosystem of EFNSAs to protect its economy, sustain its military-industrial complex, and circumvent Western financial restrictions.

EFNSAs are individuals, companies, or networks that are not formally part of the Russian state apparatus but nonetheless blur the line between public and private by directly or indirectly advancing state geoeconomic interests and sustaining its financial systems. They include actors who facilitate sanctions evasion, safeguard elite wealth, and enable covert access to capital, goods, and technologies essential to Russia's war effort and geopolitical ambitions.

Under Putin, this ecosystem has been consolidated and reoriented towards geopolitical objectives. State-aligned banks and companies have become instruments of statecraft, while oligarchs operate as intermediaries and enablers, deploying their corporate assets and international networks to serve the Kremlin's interests with plausible deniability.

This presents a unique challenge to liberal democracies, **as many of these actors operate within the framework of private enterprise and international commerce, giving them the appearance of legitimacy while quietly advancing Russian state goals.** Their embeddedness in global markets makes them difficult to isolate or deter through traditional policy tools, complicating enforcement and creating systemic vulnerabilities in Western financial systems.

This chapter examines how EFNSAs align with state interests, while also illustrating how this alignment does not always indicate direct Kremlin control, as EFNSAs often pursue actions that serve both their own interests and those of the state. It then briefly explores how several NSAs profiled in prior chapters – professional enablers, PMCs, TCNs and cybercriminals – also perform key economic and financial functions in support of the Russian state. Together, these actors form a decentralised but

coordinated architecture of sanctions resistance that challenges conventional approaches to economic warfare and national security.

Oligarchs

A relatively small group of wealthy business tycoons, known as oligarchs, have played a significant role in shaping the Russian economy in the post-Soviet era.[327] Described as "the engine of Russia's economic recovery and institutional reform",[328] oligarchs own or control many of Russia's largest corporations that are vital to state revenue, employment and strategic infrastructure. Their investment decisions, export activities and access to international capital have historically shaped the country's economic trajectory. However, oligarchs have also become synonymous with corruption due to their monopolistic control over key sectors and their exploitation of state resources for personal gain. For an explanation of how they rose to power, see **Table A3**.

During the Yeltsin presidency – a period marked by sweeping privatisation and deregulation – oligarchs were able to wield their economic power with relative independence. However, President **Putin has sought to institutionalise the relationship between state and business.** Under Putin, oligarchs are expected to "act as custodians of Russian national wealth and, when required, as arms of the state".[329] As economist William Tompson commented, "Far from being the state's master, Russian private capital was to be its servant".[330]

Putin keeps a tight leash on oligarchs' financial dealings, with almost any transaction over a certain threshold apparently requiring his approval.[331] A senior Western banker told journalist Catherine Belton in 2017 of his surprise that Putin became involved in a "mere" $20 million deal involving a businessman who wanted to sell up and leave Russia – the sale was denied.[332] Moreover, Putin has responded to any political criticism voiced by oligarchs with severe reprisals.[333]

Prior to Russia's full-scale invasion of Ukraine, oligarchs were key instruments of Russian influence abroad – leveraging their wealth, international business networks and elite access to shape political and economic environments in Western countries. Many invested heavily in real estate, media, and

327 For a comprehensive list of Russian oligarchs, see Giacomo Tognini and John Hyatt, 'The Forbes Ultimate Guide to Russian Oligarchs', Forbes, 11 April 2023, https://www.forbes.com/sites/giacomotognini/2022/04/07/the-forbes-ultimate-guide-to-russian-oligarchs/.

328 Sergei Guriev and Andrei Rachinsky, 'The Role of Oligarchs in Russian Capitalism', *Journal of Economic Perspectives, 19*(1), (2005): 131–150.

329 Matthew Redhead, 'Old Wine, New Bottles? The Challenge of State Threats', SOC ACE Research Paper 32 (University of Birmingham, January 2025), 77, https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/67852e69ff4ff4079a9c3000/1736781420568/SOCACE-RP32-OldWineNewBottles_final.pdf.

330 William Tompson, 'Putin and the "Oligarchs": A Two-Sided Commitment Problem?', in *Leading Russia: Putin in Perspective: Essays in Honour of Archie Brown,* ed. Alex Pravda (Oxford University Press, 2005), 179–203.

331 Catherine Belton, *Putin's People* (HarperCollins, 2020), 484.

332 Ibid.

333 For instance, Mikhail Khodorkovsky, once the richest man in Russia, was arrested, stripped of his oil company and spent ten years in a Siberian prison after criticising Putin for corruption. See Greg Rosalsky, 'How Putin Conquered Russia's Oligarchy', Planet Money, 29 March 2022, https://www.npr.org/sections/money/2022/03/29/1088886554/how-putin-conquered-russias-oligarchy.

strategic industries around the world, and maintained close relationships with foreign policymakers, especially in Europe.

However, since Russia's 2014 annexation of Crimea and the 2022 full-scale invasion of Ukraine, many Russian oligarchs have been personally sanctioned by the US, EU and UK, meaning they are subject to travel restrictions and their overseas assets have been frozen.[334] As a result, they can no longer effectively serve as informal ambassadors or economic agents of the state.

In response, the Kremlin appears to have reoriented the role of oligarchs inwards – from instruments of sharp power on the global stage to pillars of the domestic financial system. This shift was starkly illustrated when Putin summoned over 40 oligarchs to a meeting at the Grand Kremlin Palace on the day he ordered the invasion of Ukraine.[335] The purpose of the meeting was ostensibly for Putin to explain his reasons for the invasion, but the implicit message was clear: oligarchs must use their wealth and influence to support the war effort, and dissent from this course of action would not be tolerated. [336]

Since February 2022, Russian oligarchs have been expected to support domestic economic stability and wartime resilience. This includes funding infrastructure and military-linked projects, absorbing economic shocks through targeted investments, and maintaining employment in key sectors. **In return, they are granted continued access to state contracts, many in the defence sector.**[337] This has proved profitable, with the combined wealth of Russia's oligarchs reaching US$625.5 billion in 2025, surpassing the previous 2021 record of US$606.2 billion.[338]

However, these economic benefits are conditional on an oligarch's loyalty to the Kremlin. As one senior Russian state banker told the *Financial Times* in March 2022, "[b]eing on the U.S. sanctions list used to be a status symbol of patriotism. But now it's a requirement. If you're not on it, it's suspicious".[339] A few oligarchs have spoken out against the war, but they are generally individuals who have cut ties with Russia.[340] For Russia-based oligarchs, the penalty for stepping out of line is, at the

334 Jane Clinton and Georgina Quach, 'Russia: the oligarchs and business figures on western sanction lists', The Guardian, 10 March 2022, https://www.theguardian.com/world/2022/mar/04/russia-oligarchs-business-figures-west-sanction-lists-us-eu-uk-ukraine.

335 Max Seddon, 'Russia's oligarchs powerless to oppose Putin over Ukraine invasion', The Financial Times, 1 March 2022, https://www.ft.com/content/5cd2c951–6b23–4e07-a72d-4731f7a71b58.

336 The Bell, 'Guest list scrutiny as Putin meeting with billionaires', 21 March 2023, https://en.thebell.io/guest-list-scrutiny-as-putin-meeting-with-billionaires/.

337 Vitaly Soldatskikh et al., 'Lapdogs of War: A Guide to Russia's Wartime Oligarchs', Proekt, 2024, https://www.europeanpressprize.com/article/lapdogs-of-war-a-guide-to-russias-wartime-oligarchs/.

338 'Wealth of Russia's richest people rises to record $625.5 billion', Reuters, 17 April 2025, https://www.reuters.com/world/europe/wealth-russias-richest-people-rises-record-6255-billion-2025–04–17/.

339 Seddon, 'Russia's oligarchs powerless to oppose Putin over Ukraine invasion'.

340 Giulia Carbonaro, 'What difference do oligarchs condemning the war make for Putin's Russia?', Euronews, 16 August 2023, https://www.euronews.com/2023/08/16/what-difference-do-oligarchs-condemning-the-war-make-for-putins-russia.

very least, prosecution, imprisonment and asset forfeiture, if not death.[341]

State-aligned corporations

Under Putin, many large Russian companies have been integrated into the state apparatus, whether through formal ownership structures, patronage-based appointments, or the implicit expectation that the private sector will act in alignment with state policy. **These corporations play a central role in laundering state funds, circumventing sanctions and projecting influence abroad to advance both state and commercial interests.** There are three main sub-categories of corporate EFNSAs: state-aligned banks, major companies in strategic sectors, and importers of dual-use or sanctioned goods.

Since the full-scale invasion of Ukraine in 2022, the alignment between these corporations and state priorities has become even more explicit. As Western sanctions have intensified, many of these entities have been repurposed to sustain Russia's war economy. Just as oligarchs have been reoriented towards the Kremlin's domestic financial agenda and distanced from their previous role as international powerbrokers, so too have Russian corporations been mobilised by the state to uphold internal economic stability, finance military efforts and maintain strategic trade flows.

A. Banks

Prior to the 1990s, the state had full control over the Russian banking industry, yet following the collapse of the Soviet Union, the banking sector underwent rapid decentralisation.[342] By the end of 1996, 75% of Russian banks had been privatised.[343] Since Putin came to power in 2000, the Kremlin has steadily worked to reassert state control over the financial sector. **Under Putin's leadership the Russian banking industry has, in many respects, come full circle, with most banks once again consolidated under state ownership.**

Today, the Russian banking industry is structured into three tiers: the Central Bank of Russia (CBR), state-controlled banks, and small private banks.[344]

Small private banks best illustrate how Russia's use of commercial entities as EFNSAs is often decentralised and contradictory. A well-publicised example was the 2014 multimillion-euro loan issued by FCRB to the National Front,

341 At least eight oligarchs believed to have held anti-war views have died under suspicious circumstances since 2022. See Aleksandar Brezar and David MacDougall, 'Updated: A list of oligarchs and Putin critics found dead since Ukraine war', Euronews, 22 September 2022, https://www.euronews.com/2022/09/22/accidental-defenestration-and-murder-suicides-too-common-among-russian-oligarchs-and-putin.

342 BER staff, 'Privatization of the Banking Industry in the Russian Federation', Berkeley Economic Review, 16 March 2021, https://econreview.studentorg.berkeley.edu/privatization-of-the-banking-industry-in-the-russian-federation/.

343 Jeffery Abarbanell and Anna Meyendorff, 'Bank Privatization in Post-Communist Russia: The Case of Zhilsotsbank', *Journal of Comparative Economics*, 25(1), (1997), 62–96, https://doi.org/10.1006/jcec.1997.1448.

344 Andrei Vernikov, 'The Impact of State-Controlled Banks on the Russian Banking Sector', *Eurasian Geography and Economics*, 53(2), (2013), 250–266, https://doi.org/10.2747/1539–7216.53.2.250.

TABLE 6. Hierarchy of the Russian banking industry

CBR	State-controlled banks	Small private banks
• The CBR serves as both the principal regulator of the financial system and the dominant shareholder in most large commercial banks. • This consolidation of power enables the state to exert considerable influence over credit allocation, currency controls, and capital flows. • Through the manipulation of monetary policy and its ownership stakes, the CBR can direct lending towards strategic sectors, enforce compliance with domestic economic goals, and cushion the economy against international sanctions.	• The five largest Russian state-controlled banks are Sberbank, VTB, Gazprombank, Promsvyazbank and the Russian Agricultural Bank.[345] • Over the past two decades, most large private banks have been effectively nationalised through CBR intervention.[346] • Oligarchs still wield influence over these banks through their shareholdings and board appointments. • In turn, these banks often provide preferential credit and channel state subsidies to oligarch-controlled firms, particularly in sanctioned or strategic industries. • Since the escalation of Western sanctions, these banks have been instrumental in executing shadow financial operations – routing payments through opaque offshore entities or facilitating transactions in alternative currencies to maintain Russia's financial relations with non-Western partners.[347]	• Small private banks are often acquired by the CBR or have their licences revoked if they grow too large or stray from state expectations.[348] • However, the Kremlin appears to tolerate the existence of a small number of non-state banks to provide cover for state-aligned financial operations. • Although information about these banks' activities is rarely made public, one notable example is the First Czech Russian Bank (FCRB). • Investigative reporting uncovered FCRB's central role in the "Russian Laundromat" – a massive capital flight and money-laundering scheme that moved over $20 billion out of Russia between 2011 and 2014.[349] FCRB was also found to have financed Russian-organised crime groups and sanctioned oligarchs, as well as serving as a conduit for Russian financial influence operations in Western politics.

a French far-right political party.[350] As a private bank, FCRB offered plausible deniability to both the Russian officials and European Members of Parliament involved.[351] Shortly before the bank failed, the loan was briefly transferred to a shell company and then to an aviation firm with ties to the Kremlin.[352] Interestingly, this information only came to light because the Russian

345 Sean Ross, 'The 5 Biggest Russian Banks', Investopedia, 28 August 2024, https://www.investopedia.com/articles/investing/082015/6-biggest-russian-banks.asp.

346 Karina Orlova, 'Russia's Great Bank Takeover', The American Interest, 21 January 2018, https://www.the-american-interest.com/2018/01/12/russias-great-bank-takeover/.

347 Ben Aris, 'Economic warfare and the rise of Russia's shadow finance', BNE News, 14 March 2025, https://www.intellinews.com/economic-warfare-and-the-rise-of-russia-s-shadow-finance-371743/?source=russia.

348 Orlova, 'Russia's Great Bank Takeover'.

349 OCCRP, 'The Russian Laundromat Exposed', Organized Crime and Corruption Reporting Project, 20 March 2017, https://www.occrp.org/en/project/the-russian-laundromat-exposed/the-russian-laundromat-exposed.

350 Paul Sonne, 'A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening', The Washington Post, 27 December 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320–11e8-a275–81c671a50422_story.html.

351 As the relevant Member of the European Parliament later commented: "[w]e did not go to a state-owned bank because we knew that would make it a state matter", see Anne-Claude Martin, 'National Front's Russian loans cause uproar in European Parliament', Euractiv, 5 December 2014, https://www.euractiv.com/section/europe-s-east/news/national-front-s-russian-loans-cause-uproar-in-european-parliament/.

352 ASD Team and C4ADS, 'Illicit Influence – Part One – A Case Study of the First Czech Russian Bank', The German Marshall Fund, 2019, https://securingdemocracy.gmfus.org/first-czech-russian-bank-case-study/.

CASE STUDY 10: Gazprom's activities

While formally structured as a joint-stock company, Gazprom operates as an extension of the Russian state, with its leadership drawn largely from the ranks of former government officials. Its network of natural gas pipelines has enabled Russia to exercise leverage over foreign governments by manipulating energy flows.

The Nord Stream projects, for example, were not merely commercial ventures but strategic infrastructure designed to deepen European energy dependence on Russia while bypassing – and thus financially weakening – transit countries such as Ukraine.

Moreover, the Gazprom corporate empire is so powerful that it can function as multiple categories of NSAs simultaneously. It acts as a propaganda actor through its media holding company, Gazprom Media; as a social actor through its sporting sponsorships; and potentially even as an armed actor through its alleged affiliations with PMCs.

government agency responsible for insuring bank deposits sued the former FCRB bank manager, leading to a public court case. The fact that Russian officials facilitated the covert loan, yet the actions of other state agencies resulted in its exposure, highlights **a key paradox: while Kremlin influence over EFNSAs is wide-reaching, it is not always centralised, coherent or clearly attributable.**

B. Major companies in strategic sectors

Russian corporations in the energy, mining, defence and infrastructure sectors form the foundation of Russia's revenue base and geopolitical influence. While some of these entities are formally listed as private or semi-private companies, many are majority-owned by the Kremlin and chaired by oligarchs. These companies often enjoy preferential regulatory treatment, subsidised access to capital from state-controlled banks, and protection from foreign competition. In return, they are expected to fulfil key roles in economic policy implementation and geopolitical influence

Prior to 2022, these companies wielded significant power across Europe, generating substantial revenue from exports and serving as vehicles for Russian influence. Oil and gas firms in particular have a long history of establishing subsidiaries in Central and Eastern European countries that undermine the host nation's energy companies, while also providing a channel for illicit payments to local officials, thus entrenching Russian influence and creating a loyal circle of elites.[353] There are documented examples of such "gas intermediaries" making donations to pro-Russian politicians and political parties in Serbia, Croatia, Ukraine and the Czech Republic.[354]

Gazprom, Russia's state-owned energy giant and the world's largest extractor of natural gas, exemplifies how the Kremlin uses EFNSAs to advance its geopolitical agenda under the guise of commercial activity (see **Case Study 10**).[355]

353 Tena Prelec, 'Russian IFF and political influence in South Eastern Europe: How financial flows and politics intersect in Montenegro and Serbia', SOC ACE Briefing Note 8 (University of Birmingham, May 2022), https://www.socace-research.org.uk/publications/russian-iff-south-eastern-europe-bn8.

354 Catherine Owen, Tena Prelec and Tom Mayne, 'The Illicit Financialisation of Russian Foreign Policy', SOC ACE Research Paper 3 (University of Birmingham, May 2022), 16–17, https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/6481ed0061707e40ea865aad/1686236417031/SOCACE-RP03-Illicit_Financialisation-Jun23.pdf; Neil MacFarquhar, 'How Russians Pay to Play in Other Countries', The Washington Post, 30 December 2016, https://www.nytimes.com/2016/12/30/world/europe/czech-republic-russia-milos-zeman.html.

355 See Vladimir Milov, 'How Gazprom Manipulated the EU Gas Market', Wilfried Martens Centre for European Studies, 3 February 2022, https://www.martenscentre.eu/blog/how-gazprom-manipulated-the-eu-gas-market/; Samantha Gross and Constanze Stelzenmuller, 'Europe's messy Russian gas divorce', Brookings, 18 June 2024, https://www.brookings.edu/articles/europes-messy-russian-gas-divorce/; Stefan Hedlund, 'The rise and fall of Russia's Gazprom', Geopolitical Intelligence Services, 25 July 2024, https://www.gisreportsonline.com/r/gazprom-russia-europe-eu-gas/; 'Gazprom Media', Media & Journalism

Since the annexation of Crimea in 2014 and, to a greater extent, the full-scale invasion of Ukraine in 2022, Russian firms have been forced to take on greater domestic economic stabilisation functions. As Western financial sanctions have increasingly targeted state-linked corporations and their leadership, companies in strategic sectors have pivoted towards alternative markets, such as China, India, Türkiye, and the Middle East.[356] Gazprom again provides a clear example of this transition. Once the supplier of 40% of Europe's imported natural gas, Gazprom's market share shrank to just 9% after the invasion, and the Kremlin barred it from paying dividends for 2023 after the company suffered its first annual loss since 1999.[357] Yet in 2024, Gazprom rebounded with a net profit of 1.2 trillion roubles,[358] driven by increased exports to China, currency stabilisation and higher interest income.[359] Structural vulnerabilities persist, including the loss of key pipeline routes, but Gazprom's trajectory illustrates how corporate EFNSAs have been repurposed to support Russia's economic resilience in the face of unprecedented Western sanctions.

C. Importers of dual-use goods

Despite Putin's 2023 pledge to make Russia a "self-sufficient state",[360] the Kremlin remains unable to sustain its military-industrial complex entirely through domestic production. As Western sanctions have deepened, Russia has increasingly come to rely on an ecosystem of importers, front companies, and logistical intermediaries to obtain critical "dual-use goods" – items with both civilian and military applications, including semiconductors, microchips and drone components.[361] These

Research Center, 26 September 2024, https://statemediamonitor.com/2024/09/gazprom-media/; Tony Wesolowsky, 'After getting the red card from UEFA, Gazprom is getting back in the sports sponsorship game', RadioFreeEurope, 11 May 2024, https://www.rferl.org/a/gazprom-uefa-ferencvaros-hungary-soccer-ukraine-war-schalke/32941442.html; Serhii Nuzhnenko, 'It's not just Wagner. At least three Gazprom-linked private military companies now have fighters in Ukraine', Meduza, 16 May 2023, https://meduza.io/en/feature/2023/05/16/it-s-not-just-wagner.

356 Arthur Sullivan, 'How has Russia's economy dodged Western sanctions', Deutsche Welle, 22 February 2025, https://www.dw.com/en/sanctions-russian-economy-could-no-longer-survive-without-china-india-and-turkey/a-71606396.

357 Victor Jack, 'How Putin has maimed Gazprom', Politico, 16 October 2022, https://www.politico.eu/article/russia-vladimir-putin-wounds-gazprom-ukraine-war-natural-gas-lng-energy/; 'Russian government tells loss-making Gazprom not to pay dividends for 2023', Reuters, 20 May 2024, https://www.reuters.com/business/energy/russian-government-tells-loss-making-gazprom-not-pay-dividends-2023–2024–05–20/.

358 About 1.2 billion euros.

359 'Russia's Gazprom returns to annual profit in 2024, earning $14.8 billion', Reuters, 30 April 2025, https://www.reuters.com/business/energy/russias-gazprom-returns-annual-profit-2024-earning-148-billion-2025–04–30/.

360 'Putin Vows to Make Russia "Self-Sufficient" in Fifth Term', VOA News, 17 December 2023, https://www.voanews.com/a/putin-vows-to-make-russia-self-sufficient-in-fifth-term/7402117.html.

361 Tom Keatinge, 'Developing Bad Habits: What Russia Might Learn From Iran's Sanctions Evasion', RUSI Occasional Paper (RUSI, June 2023), https://static.rusi.org/developing-bad-habits-what-russia-might-learn-from-irans-sanctions-evasion.pdf.

networks form the backbone of Russia's efforts to maintain military-industrial capacity under sanctions. While they do not always operate under formal command structures, their alignment with Kremlin objectives reflects the decentralised yet state-aligned nature of many EFNSAs.

Importers of dual-use goods typically operate through jurisdictions with weak export controls, legal opacity and neutral or friendly trade relationships with Russia. These conditions make such supply chains inherently difficult to trace, but the scale of the activity can be inferred from the sharp increase in exports of Western goods. For instance, the countries of the Balkans, Caucasus, and Central Asia, as well as Türkiye and the UAE, collectively increased their imports of European and American goods by US$133 billion in 2022–2023.[362] The exponential surge strongly suggests that many companies in these jurisdictions are acting as conduits for Russian procurement.

Oligarch-linked firms are frequently involved in these operations, leveraging offshore corporate structures and trade networks to obscure end users and re-export sensitive goods back to Russia.[363] For example, investigations have uncovered shell companies in Dubai and Hong Kong that act as procurement agents for Russian military contractors to obtain sanctioned military technology.[364] The use of nominally private individuals and companies for this purpose allows the Russian government to deny direct involvement, shifting culpability to private actors operating in legal "grey zones".

A prominent example is Russia's use of its **"shadow fleet"** – a rapidly expanding group of aging, reflagged, and poorly insured tankers that operate outside of traditional maritime tracking systems to transport restricted commodities, most notably crude oil.[365] While the concept has been used by other sanctioned regimes such as Iran, North Korea, and Venezuela, the scale, sophistication and geopolitical implications of Russia's illicit maritime network are unprecedented.[366] Reports estimate that the Kremlin has spent approximately US$10 billion since 2022 on building and maintaining

362 JAM News, 'Chip up the sleeve: How Russia sidesteps sanctions', JAM News, 29 April 2024, https://jam-news.net/chip-up-the-sleeve-how-russia-sidesteps-sanctions/.

363 'As Russia feels effects of multilateral sanctions campaign, Treasury takes further action against Russia's international supply chains', US Department of the Treasury, 23 August 2024, https://home.treasury.gov/news/press-releases/jy2546.

364 Frank Millard, Jonathan Swift and Niall McCrae, 'Why the UAE is Becoming a Liability: The Case of Russian Sanctions Evasion', Tactics Institute for Security & Counter Terrorism, 2004, https://tacticsinstitute.com/reports/why-the-uae-is-becoming-a-liability-the-case-of-russian-sanctions-evasion/; Aaron Krolik and Paul Mozur, 'How US Chips Continue to End Up in Russian Missiles', The New York Times, 25 July 2024, https://www.nytimes.com/2024/07/25/technology/russia-sanctions-chips.html.

365 European Parliament, 'Russia's 'shadow fleet': Bringing the threat to light', European Parliamentary Research Service Briefing (European Parliament, November 2024), https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)766242.

366 Gonzalo Saiz, 'RUSI Maritime Sanctions Taskforce: First Meeting Report', RUSI Conference Report (RUSI, December 2024), https://static.rusi.org/maritime-sanctions-taskforce-conference-report.pdf; Gonzalo Saiz, 'RUSI Maritime Sanctions Taskforce: Second Meeting Report', RUSI Conference Report (RUSI, March 2025), https://static.rusi.org/maritime-sanctions-taskforce-second-conference-report.pdf.

its shadow fleet.[367] By mid-2024, shadow vessels were transporting an estimated 4.1 million barrels of Russian crude oil every day,[368] fundamentally undermining the G7 oil price cap and enabling Russia to continue generating substantial energy revenues in defiance of sanctions.

Sanctions evasion enablers

As outlined above, EFNSAs play a fundamental role in enabling sanctions evasion, now that circumventing Western financial sanctions has become a central objective of the Kremlin. In addition to domestic actors, the Russian state has increasingly relied on non-Russian EFNSAs to sustain its economy. Foreign banks, businesses and intermediaries have played a critical role in circumventing sanctions, sustaining trade, and laundering funds. Prior to 2022, banks in Latvia, Estonia, the Netherlands and Austria, among others, were investigated for serving as conduits for Russian capital.[369] While many of these European countries have since undertaken significant reforms to effectively enforce sanctions,[370] Chinese financial institutions and professional service providers continue to facilitate Russian access to global markets and critical technologies.[371] These external EFNSAs offer the Kremlin strategic flexibility, enabling it to project economic influence and resilience without direct state involvement or exposure.

Additionally, Russia relies on a wide array of entities not traditionally classified as EFNSAs, such as PMCs, TCNs and cybercriminals, but which nonetheless facilitate sanctions circumvention, money-laundering activities and economic sabotage. These entities are examined in greater detail in the chapters on ANSAs and CNSAs. The financial and economic dimensions of these NSAs are briefly outlined here, with the important caveat that this overview is intended to complement the more detailed analysis provided in the dedicated chapters for each NSA category.

A. Lawyers and professional service providers
Professional service providers – particularly lawyers, accountants, wealth managers and company formation agents – play a pivotal role in shielding the wealth and activities of the Russian elite from scrutiny. These so-called "professional enablers" are instrumental in

367 Benjamin Hilgenstock et al., 'Creating "Shadow-Free" Zones: Proposal for the Implementation of an Insurance Requirement to Address Key Environmental Risks', KSE Institute Report (KSE Intitute, October 2024), https://sanctions.kse.ua/wp-content/uploads/2024/10/Shadow_free_zones_October_2024_final.pdf.
368 Ibid.
369 'Factbox: European banks hit by Russian money laundering scandal', Reuters, 8 March 2019, https://www.reuters.com/article/business/factbox-european-banks-hit-by-russian-money-laundering-scandal-idUSKCN1QP1P2/.
370 For instance, since 2019, Latvia has passed strict anti-money laundering laws, implemented client screening processes for banks, and established a financial intelligence unit. See Koen Verhelst, 'How dirty Russian money taught Latvia to get serious on sanctions', Politico, 10 May 2024, https://www.politico.eu/article/latvia-designated-financial-intelligence-unit-enforcing-sanctions-imposed-eu-response-russia-dirty-money/.
371 Piotr Dzierzanowski and Marcin Przychodniak, 'China's Economic Support for Russia Since the Full-Scale Invasion of Ukraine', PISM Report (Polish Institute of International Affairs, February 2025), https://www.pism.pl/publications/chinas-economic-support-for-russia-since-the-full-scale-invasion-of-ukraine.

structuring opaque financial arrangements that obscure the ownership and origin of assets.[372] Common sanctions-evasion tactics include creating complex offshore networks involving trusts, shell companies, and special purpose vehicles located in permissive jurisdictions such as the British Virgin Islands, Cyprus, and Switzerland.[373] These structures allow sanctioned individuals to move capital, purchase property, and maintain access to Western financial markets without detection. Lawyers also engage in what is known as "lawfare", the strategic use of litigation not only to silence critics and investigative journalists, but also to delay or prevent asset seizures by Western authorities. These legal challenges are often made within Western legal systems, creating a paradox whereby democratic institutions are used to protect autocratic wealth.[374]

Since 2022, sanctions have increasingly targeted professional enablers, alienating Russian clients from Western professional service providers.[375] Yet demand for their services has only grown, as Russian oligarchs and state-aligned corporations seek new ways to protect their assets. Legal firms in the UAE, China, Türkiye, and post-Soviet states have become key players in restructuring corporate ownership, registering alternative citizenships, and creating financial channels outside the Western sphere.[376] Thus, while not EFNSAs in the traditional sense, these enablers function as critical cogs in the machinery of Russian sanctions evasion.

B. Private military companies

PMCs intersect with EFNSAs through their role as facilitators of covert economic extraction. While officially independent entities, these groups receive support from the RIS and provide the Kremlin with plausible deniability in operations across resource-rich conflict zones. PMCs have been deployed to prop up Russian-aligned regimes and secure access to strategic commodities, such as gold mines in Sudan and oil assets in Libya.[377] These operations often involve securing economic concessions or engaging in barter-style arrangements whereby security services are exchanged for direct access to extractive revenues.[378] The profits

372 'Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes', OECD Report (OECD, 2021), https://www.oecd.org/en/publications/ending-the-shell-game_79e22c41-en.html.

373 Justyna Gudzowska, Eliza Lockhart and Tom Keatinge, 'Disabling the Enablers of Sanctions Circumvention', RUSI Policy Brief (RUSI, May 2024), https://www.rusi.org/explore-our-research/publications/policy-briefs/disabling-enablers-sanctions-circumvention.

374 Jim Fitzpatrick, 'MPs slam top "lawfare" firm for keeping finances secret', openDemocracy, 14 December 2022, https://www.opendemocracy.net/en/carter-ruck-cms-harbottle-lewis-schillings-profits-secret/.

375 Per Vestergaard Pedersen and Stine Gellert, 'Sanctions rules prohibiting the provision of certain services to Russian companies, including Russian subsidiaries', DLA Piper, 19 June 2024, https://denmark.dlapiper.com/en/news/sanctions-rules-prohibiting-provision-certain-services-russian-companies-including-russian.

376 National Crime Agency, 'Financial Sanctions Evasion Typologies: Russian Elites and Enablers', Red Alert Report, (National Crime Agency, July 2022), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/605-necc-financial-sanctions-evasion-russian-elites-and-enablers/file.

377 R. Kim Cragin and Lachlan MacKenzie, 'Russia's Escalating Use of Private Military Companies in Africa', Institute for National Strategic Studies, 24 November 2020, https://inss.ndu.edu/Media/News/Article/2425797/russias-escalating-use-of-private-military-companies-in-africa/.

378 Brian Katz et al., 'Moscow's Mercenary Wars', Center for Strategic & International Studies, September 2020, https://russianpmcs.csis.org/.

generated through these overseas ventures are funnelled back to Russia through opaque financial channels, often using front companies registered in the UAE.[379]

The role of PMCs underwent a significant transformation after 2022, as the Russian state increasingly centralised control over the war effort in Ukraine. Some elements of Wagner and other PMCs have persisted (albeit under tighter state control or rebranding) and remain active in Africa, where resource extraction continues to fund both Kremlin-aligned actors and broader geopolitical influence campaigns. These operations are often facilitated by oligarch-linked firms that handle the procurement, shipping and resale of extracted resources, thereby embedding paramilitary activity within broader sanctions-evasion and money-laundering networks.

C. Transnational criminal networks

Russian TCNs are integral to the country's economy. They specialise in illicit trade, smuggling, and money laundering – skills that closely align with the Kremlin's need to move restricted goods and funds across international borders without detection. TCN operations increasingly blur the line between criminality and Russian statecraft, with TCNs maintaining a flexible relationship with the RIS while also, as alleged by a 2024 UK law enforcement investigation, providing the "black cash" funds for Russian intelligence operations.[380] TCNs' expertise in black-market logistics makes them uniquely positioned to operate in high-risk environments and evade international regulatory regimes.

The imposition of sweeping Western sanctions has only increased the utility of TCNs to the Russian state. As RUSI Senior Associate Fellow Mark Galeotti observed, "[s]ince the 2022 invasion of Ukraine… the conscription state has shifted into a full 'mobilisation state' in which all elements of society – illegal as well as legal – are expected to play their full part in the war".[381]

In particular, TCNs have become central to the covert procurement of sanctioned technologies and military-grade components, working alongside state-linked importers and corrupt foreign intermediaries.[382] Illicit supply chains now move dual-use goods from third countries into Russia, often concealed among legitimate cargo such as washing machines and refrigerators.[383] These activities not only finance the war effort but also help preserve the illusion of economic normalcy within Russia, reinforcing the state's resilience strategy.

D. Cybercriminals

Russia's cybercriminal ecosystem constitutes a dynamic and adaptive network of actors that have historically operated in a tolerated

379 Olivia Allison et al., 'Wagner's Business Model in Syria and Africa: Profit and Patronage', RUSI Occasional Paper (RUSI, 6 February 2025), https://www.rusi.org/explore-our-research/publications/occasional-papers/wagners-business-model-syria-and-africa-profit-and-patronage.

380 Jamie MacColl and Kathryn Westmore, 'Operation Destabilise: Russia, Organised Crime and Illicit Finance', RUSI Commentary, 6 December 2024, https://www.rusi.org/explore-our-research/publications/commentary/operation-destabilise-russia-organised-crime-and-illicit-finance.

381 Mark Galeotti, 'Gangsters at War', 7.

382 Ibid, 20–22.

383 Ibid.

or semi-directed capacity under Kremlin oversight.[384] Cybercrime has existed since the advent of the internet, but the emergence of cryptocurrency in the late 2010s enabled criminals to anonymously generate enormous revenue from ransomware – an activity that, over the subsequent decade, has evolved into a semi-professionalised industry.[385] Although ostensibly independent criminal enterprises, these groups often refrain from targeting Russian systems and have been suspected of cooperating with the RIS on an ad hoc basis.[386] **Since 2022, cybercriminals have escalated their activities in tandem with Putin's broader economic and geopolitical goals.** There has been a notable rise in cyberattacks on NATO member-state infrastructure, banks, logistics networks, and government agencies.[387] These operations are no longer purely financially motivated but are increasingly integrated into the broader Russian strategy of infrastructure sabotage, disinformation campaigns, and asymmetric warfare.[388] Cryptocurrency theft, digital extortion, and data breaches continue to generate income for sanctioned cyber actors, while the attacks hinder Western coordination and sanctions enforcement. **In effect, cybercriminals now operate as agents of strategic economic disruption – making them a critical, albeit unofficial, component of Russia's geoeconomic architecture.**

384 Redhead, 'Old Wine, New Bottles? The Challenge of State Threats', 84–5.

385 Jamie MacColl and Gareth Mott, 'Organised Cybercrime: The Rise of Ransomware as a National Security Threat', RUSI Commentary, 13 December 2023, https://www.rusi.org/explore-our-research/publications/commentary/organised-cybercrime-rise-ransomware-national-security-threat.

386 Keir Giles, *Russia's War on Everybody: And What It Means for You* (London: Bloomsbury Academic, 2023), pp. 203–4; Matt Burgess, 'Leaked Ransomware Docs Show Conti Helping Putin From the Shadows', Wired, 10 March 2022, https://www.wired.com/story/conti-ransomware-russia/.

387 Victor Jack, 'UK warning: Russia's "aggressive" cyber warfare is threat to NATO', Politico, 24 November 2024, https://www.politico.eu/article/russias-aggressive-cyberattack-putin-poses-threat-nato-uk/.

388 Anna Maria Dyner, 'Russia Continuing Cyberthreats Against NATO Countries', The Polish Institute of International Affairs, 21 November 2023, https://pism.pl/publications/russia-continuing-cyberthreats-against-nato-countries.

Russian state institutions behind non-state actors

By Eliza Lockhart and Eginhards Volāns

When analysing how the Russian regime leverages NSAs to advance its objectives, it can be tempting to try to identify a "master plan". As the work of international relations scholar Robert Jervis illustrates, **governments often overestimate the degree of coherence and coordination behind their adversaries' actions.**[389] Research by RUSI Senior Associate Fellow Matthew Redhead[390] highlights that **this tendency is especially pronounced when democratic governments assess the threats emanating from authoritarian regimes.**

In such cases, there is often an assumption of centralised authority, top-down decision-making and absolute control being exercised by a single leader. Yet, as political scientist Barbara Geddes and colleagues have shown, **decision-making processes within dictatorships can be just as fragmented as within democracies.**[391]

Analysts differ in their assessments of Putin's system of governance, ranging from portrayals of firm hierarchical control to descriptions of loosely coordinated chaos.[392] In reality, both dynamics appear to coexist. While the decision to initiate hostile activities is typically centralised within the RIS, the execution of these acts often unfolds through a less-than-functional mix of state and non-state actors. This has resulted in NSAs frequently being labelled as "proxies", implying direct state control. However, **in the murky realm of covert operations, establishing a clear chain of command between state and non-state actors is often unfeasible.**

As Redhead articulates, perhaps the most that can be hoped for is to collect enough material to:

a) identify a probable relationship between a state and a non-state actor, and
b) find consistency and alignment between the state actor's objectives and the apparent objectives of the non-state actor's conduct.[393]

Even then, such alignment does not necessarily imply a clear nexus – **NSAs may act in ways that advance state interests for independent reasons.** Moreover, in an environment where loyalty to Putin is paramount and suspicion of disloyalty is rife, it is not uncommon for various NSAs to try to anticipate what Putin wants, without necessarily receiving direct orders.[394]

As such, identifying the specific state entities that might influence or control NSAs requires care. With this caveat in mind, **Table 7** lists the Russian state institutions that regularly interact with the various types of NSAs discussed in previous chapters of the handbook. The links between these NSAs and Russian state institutions are shown in **Figure A3**.

389 Robert Jervis, *Perception and Misperception in International Politics* (New Jersey: Princeton University Press, 1976).
390 Redhead, 'Old Wine, New Bottles? The Challenge of State Threats'.
391 Barbara Geddes, Joseph Wright and Erica Frantz, *How Dictatorships Work* (Cambridge University Press, 2018).
392 Andrew Monaghan, *Power in Modern Russia: Strategy and Mobilisation* (Manchester: Manchester University Press, 2017).
393 Redhead, 'Old Wine, New Bottles? The Challenge of State Threats', p. 75.
394 Mikhail Zygar, *All the Kremlin's Men: Inside the Court of Vladimir Putin* (PublicAffairs, 2016).

TABLE 7. Russian state institutions involved in the orchestration of NSAs[395]

State institution	Cyber NSAs	Propaganda and disinformation NSAs	Social and political NSAs	Armed NSAs	Economic and financial NSAs
Presidential Administration (PA)		The PA is central to the development and orchestration of various types of PDNSAs. Several departments and high-ranking officials are directly involved in this process. **Sergey Kiriyenko** and subordinates manage the **SDA** (a PR agency responsible for global-scale information operations). Kiriyenko is also linked to several **NPOs** used to finance internal propaganda projects and oversees the Russian internet segment. Additionally, he has reportedly expanded his influence in Africa, and his role has grown significantly since the full-scale invasion of Ukraine. **Aleksei Gromov** and his subordinates have historically been in charge of **traditional propaganda** (e.g. television). Additionally, structures such as the **Directorate for Interregional Relations and Cultural Contacts with Foreign Countries** are involved in orchestrating PDNSAs in post-Soviet states.	There is no clear distinction between the orchestration of PDNSAs and SPNSAs in the PA. The **Directorate for Cross-Border Co-operation** and the **Directorate for Interregional Relations and Cultural Contacts with Foreign Countries** have historically been involved in orchestrating various SPNSAs to advance the Kremlin's geopolitical goals. Directorates were abolished in late August 2025 and likely integrated into a newly established **Directorate for Strategic Partnership and Cooperation**. These directorates have strong ties to the **FSB** and **SVR**, essentially working in tandem to establish networks of influence through agents, NGOs, think tanks, media projects and even some pro-Kremlin politicians. **Dmitry Kozak** was previously in charge of post-Soviet countries, but following the invasion of Ukraine, his role diminished, and he was dismissed from his duties by September 2025.		The PA is the main centre of strategic planning and oversight for EFNSA activities, including oligarchs, strategic investments, political influence activities and economic operations abroad.

395 The information presented in this table does not claim to represent the objective or comprehensive truth. It draws on publicly available, yet often limited, sources and should be considered indicative of the situation. The table focuses on identifying observable ties between NSAs and state institutions without assessing the depth, nature, or degree of state control over these actors. Furthermore, the relationships mentioned in the table are likely only a partial reflection of the far more complex ecosystem of the Russian state and NSAs. Readers are therefore encouraged to interpret this information with caution and to treat it as a starting point for further inquiry rather than a comprehensive account.

State institution	Cyber NSAs	Propaganda and disinformation NSAs	Social and political NSAs	Armed NSAs	Economic and financial NSAs
Federal Security Service (FSB)	The FSB controls several-linked hacking groups, including **Turla**, **Gamaredon**, and **Callisto**. In addition, the FSB has historically maintained close ties with the **cybercriminal underworld**, which it has utilised either to recruit new hackers or blackmail them into supporting state objectives. The FSB is closely linked to several **scientific research centres** and **private IT companies**, which are used to support the Russian cyber programme.	The FSB's **5th Service** is known for orchestrating influence operations abroad and, more widely, for intelligence failures before the invasion of Ukraine. The FSB's **2nd Service** has reportedly been involved in orchestrating similar influence operations. Additionally, the FSB is known to operate proxy websites such as **South Front and News Front**. Following the Wagner Group's failed mutiny in 2023, the FSB began operating PDNSAs in Africa, including the **African Initiative**.	The FSB's **5th Service** is involved with SPNSAs operating within the Russian compatriot community abroad. Additionally, the FSB is known to establish ties with foreign politicians for espionage or influence purposes.	The FSB is highly involved in orchestrating multiple subcategories of ANSAs. It has deeply rooted ties with TCNs and contract killers, as evidenced by the cases of **Vadim Krasikov** and **Jan Marsalek**. Additionally, the FSB has established relationships with some PMCs, such as the **RSB Group**, and various militias, paramilitaries and terrorist groups, often with far-right ideological leanings.	The FSB is responsible for the domestic coordination of money-laundering operations, often through TCNs, as well as sanctions evasion and financial surveillance.
Foreign Intelligence Service (SVR)	Compared to its counterparts, the FSB and GRU, less is known about the SVR's cyber programme. The SVR is known to operate only one state-controlled hacking group, **APT29**. Nevertheless, it is one of the most sophisticated and advanced CNSAs at Russia's disposal. The SVR's cyber operations are mainly aimed at espionage rather than disruption.	The SVR operates several PDNSAs, including **The Strategic Culture Foundation, New Eastern Outlook**, and **Oriental Review**. The SVR's front organisation, **Myrotvorets**, is also used to orchestrate disinformation operations.	The SVR works closely with various human-rights and compatriot organisations such as **Pravfond**. Additionally, it has strong links to think tanks, such as the **Russian Institute for Strategic Studies**.		The SVR manages foreign proxies, economic espionage, and legal and financial intermediaries abroad. It works in parallel with the GRU, especially when missions involve financial infrastructure or covert economic disruption.

State institution	Cyber NSAs	Propaganda and disinformation NSAs	Social and political NSAs	Armed NSAs	Economic and financial NSAs
Main Directorate of the General Staff (GRU)	The GRU operates several state-controlled hacking groups, including **Sandworm**, **APT28**, and **Ember Bear**. It is also possible that the GRU has supported or even operated the Belarus-linked group **Ghostwriter**. Additionally, the GRU is known to have close ties with the pro-Russian **hacktivist community**, influencing or outright guiding it. Since 2022, GRU-linked CNSAs are deeply involved in the war against Ukraine. Several major cyberattacks occurred before and during the invasion, including one targeting Viasat's KA-SAT satellite network, which suggests close coordination and planning with the military.	The GRU is known to operate a vast network of **proxy websites** linked to its front organisations, the **Institute of Russian Diaspora** and **InfoRos**. The **72nd Special Service Centre** plays a key role in these matters. Additionally, the GRU is known to operate networks of **Telegram** channels. The GRU has absorbed PDNSAs previously linked to the Wagner Group, such as the **Internet Research Agency**, which is now likely operated by another GRU front organisation, **the Centre for Geopolitical Expertise**.	The **72nd Special Service Centre** is involved with SPNSAs operating within the Russian compatriot community abroad.	The GRU has significant ties to various PMCs, including the most well-known successors of the **Wagner Group – Redut** and **Africa Corps**. Additionally, the GRU has ties to paramilitary groups and militias, which are often interlinked with PMCs. Reporting suggests a relationship with TCNs as well as contract killers. The GRU has also established ties to transnational jihadist groups. After 2022, the GRU appears to be the primary RIS responsible for operating disposable agents.	The GRU oversees PMCs and state-controlled hacking groups used in economic espionage targeting Western financial institutions.
Ministry of Defence (MoD)	The state-owned defence conglomerate **Rostec** is likely involved in supporting Russia's cyber programme through its subordinate scientific research centres and IT companies.	The MoD controls several PDNSAs, including radio and television channels, as well as a printed press and a film studio, primarily through its media-holding company, **Zvezda**.	The MoD has close ties to the **Russian Orthodox Church**, as indicated by the presence of Orthodox priests during Russia's hybrid and conventional war operations.	The MoD has significantly increased its influence over various PMCs, particularly since the invasion of Ukraine and the failed mutiny by the Wagner Group. The MoD's activities in this regard need to be analysed jointly with those of the GRU.	

State institution	Cyber NSAs	Propaganda and disinformation NSAs	Social and political NSAs	Armed NSAs	Economic and financial NSAs
National Guard				Some ANSAs, such as the remnants of **the Wagner Group** or parts of **the Kadyrovtsy**, are formally integrated into the National Guard.	
Ministry of Foreign Affairs (MFA)			The MFA is the supervisory institution for the **Rossotrudnichestvo** federal agency, which in turn acts as an orchestration entity for many SPNAs, especially sharp power and compatriot organisations. Rossotrudnichestvo works closely with intelligence officers, who are often stationed in **Russian Houses** abroad.		The MFA protects Russian economic interests by negotiating trade agreements and lobbying multilateral organisations. It provides diplomatic cover for EFNSAs and engages in back-door diplomacy to support state-linked companies and oligarchs.
Ministry of Culture (MoC)		The MoC plays a vital role in overseeing and subsidising the Russian film industry through the **Cinema Fund**.			
Ministry of Finance (MoF)					The MoF plays a central role in managing state funds and redirecting economic flows after sanctions. It allocates state subsidies and loans to state-linked energy suppliers and oligarch-owned companies. The MoF works closely with the CBR.

State institution	Cyber NSAs	Propaganda and disinformation NSAs	Social and political NSAs	Armed NSAs	Economic and financial NSAs
Central Bank of Russia (CBR)					The CBR manages Russia's financial reserves and foreign-exchange operations. It designs and implements policies to counter the impact of Western sanctions and facilitates currency manipulation and alternative payment systems.
Russian Direct Investment Fund (RDIF)					The RDIF is a state-run sovereign wealth fund used to secure foreign investment and to fund strategic projects. It facilitates indirect access to Western capital markets despite sanctions.
State Duma		The State Duma operates a television channel, **DUMA TV**.	The State Duma is known to host various inter-parliamentary cooperation formats that can be used to influence foreign politicians and political parties. Since the invasion of Ukraine, the focus of parliamentary cooperation has shifted from Euro-Atlantic countries to the so-called Global South. Political parties represented in the State Duma often act as conduits of influence, establishing bilateral ties and even signing cooperation agreements with foreign political actors.		

Conclusions and knowledge gaps

Russia's use of NSAs in hybrid threats is an ever-evolving challenge that continues to shape the modern-day threat landscape faced by democratic states. These actors, often employed or orchestrated by Russia, operate in the blurred space between state and non-state, legal and illegal, and their shifting and fluid nature demands constant re-evaluation by Western governments.

Fully understanding their role in hybrid threats requires not only mapping their activities but also recognising how democracies perceive and interpret them. Western analysis often risks oversimplifying the issue, particularly by: (1) over-homogenising Russia's use of NSAs; (2) underestimating their complexity; (3) failing to account for the contextual specificities of the operational domains in which they operate; (4) disproportionately focusing on high-profile cases while overlooking less visible actors; and (5) forcing Russian behaviour into Western frameworks, thereby obscuring Russia's distinct strategic culture.

Russia's use of NSAs, while often enabled and supported by the state, rarely reflects a coherent grand strategy. Instead, it highlights the opportunism, improvisation, and idiosyncrasies that characterise Russian foreign and defence policy as a whole. The regime's inherent ambiguity makes the issue even more challenging to grasp fully, and therefore harder to counter effectively.

Looking ahead, anticipating how NSA-related threats will evolve is essential. To effectively track the ever-changing NSA threat landscape, democracies must deepen their understanding of the actors themselves, pay greater attention to overlooked domains in which they operate, and actively seek out new categories of NSAs that Russia may be using or exploiting. Additionally, an in-depth examination of the connections between these actors and the Russian state, as well as the internal systemic changes occurring within Russia, is required.

Effective countermeasures can only be implemented by gaining a comprehensive and shared understanding of the threat among Western democracies and their democratic allies. It is a lengthy, complex, and seemingly never-ending process, but one that is crucial for building resilience against hybrid threats.

To enhance understanding of NSA-related threats, this handbook not only provides a unified and comprehensive overview of the threat landscape but also highlights significant knowledge gaps identified during the research process. Addressing these gaps is essential for developing the heightened awareness required to devise future strategies that effectively counter threats posed by NSAs. These knowledge gaps should be addressed in future research and policy initiatives:

- Lack of transparency in Russia's decision-making process requires further research to understand how the state controls, influences or manipulates the various NSAs at its disposal. A more in-depth understanding is needed of how the Russian decision-making process operates in practice.
- The degree of direct control that the Kremlin exercises over NSAs remains unclear, as the

distinction between *control, delegation, cooperation, tolerance*, and *manipulation* is often blurred by design. Greater clarity and concreteness are needed to define state control and the various relationships that can exist between NSAs and the state.

- As Euro-Atlantic vigilance against Russian hybrid threats has increased since the invasion of Ukraine, and the activities of some Russia-linked NSAs have been constrained, there is a growing need to identify how Russia is adapting and leveraging new forms of NSAs to exploit vulnerabilities in democratic systems.
- The lines between the Russian state's cyber programme and cybercriminals have become increasingly blurred, requiring further examination. The extent of coordination between various CNSAs, and the role of the Presidential Administration in managing them, remains unclear and warrants further investigation. Russia's close security ties with like-minded countries, including Belarus, the DPRK, and Iran, should also be closely monitored, as these ties have the potential to extend into the cyber domain. Further research is likewise required on the recruitment and development of "cyber talent" through universities, IT companies and hacking competitions.
- As modern information operations rely heavily on IT infrastructure, there is a need for closer examination of the links between IT service providers and the Russian state, or PDNSAs acting on the Kremlin's behalf. The overall scale, level of control, and hierarchy of the Russian propaganda and disinformation ecosystem remain poorly understood and require further scrutiny. The relationship between Russia and social media platforms such as Telegram also warrants closer investigation. It is equally important to monitor any possible cooperation or coordination in the field of propaganda and disinformation between Russia and other hostile hybrid threat state actors.
- Additional research is needed on how the ideological stances of certain political parties or individual politicians may be influenced by Russia to affect their voting behaviour on Russia-related legislation. Further investigation is needed into the various lobbying organisations active across Euro-Atlantic states that present themselves as NGOs while concealing their ties to Russia and their true objectives.
- The full extent of Russia's use of alternative payment systems and its level of economic coordination with other hostile states remain insufficiently mapped and require deeper exploration. Similarly, there is limited visibility into the degree of control Russia exercises over TCNs in their role as enablers of sanctions evasion. Understanding these financial mechanisms and arrangements would help disrupt critical revenue streams for the Russian war effort. There is also a need to identify the financial intermediaries that are vital to foreign interference in democratic processes. Lastly, the role of cybercriminals in executing financial sabotage remains murky, and clearer links between state policy and cyber-economic attacks must be established.

Recommended reading

Armed NSAs

- All Eyes on Wagner, blog, https://alleyesonwagner.org/home-2/about/.
- Global Initiative Against Transnational Organized Crime, https://globalinitiative.net.
- Mark Galeotti, In Moscow's Shadows, podcast, https://inmoscowsshadows.buzzsprout.com/.
- Seth Jones, '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.
- New America's Future Frontlines, https://uncoveringwagner.org.
- Kacper Rekawek, Thomas Renard, and Bàrbara Molas, eds., *Russia and the Far-Right: Insights from Ten European Countries* (ICCT Press, 2024).
- Uğur Ümit Üngör, *Paramilitarism: Mass Violence in the Shadow of the State* (Oxford University Press, 2020).

Cyber NSAs

- Andrei Soldatov and Irina Borogan, 'Russian Cyberwarfare: Unpacking the Kremlin's Capabilities', CEPA, September 2022, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.
- Google Threat Analysis Group, blog, https://blog.google/threat-analysis-group/.
- Janne Hakala, Jazlyn Melnychuk, 'Russia's Strategy in Cyberspace' (NATO StratCom COE, June 2021).
- Microsoft Threat Intelligence, blog, https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/.
- The Recorded Future, Insikt Group, https://www.recordedfuture.com/research/insikt-group.
- Tim Mauer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge University Press, 2018).

Propaganda and disinformation NSAs

- Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (Public Affairs, 2015).
- Atlantic Council's Digital Forensics Lab, https://dfrlab.org/.
- EUvsDisinfo, https://euvsdisinfo.eu/.
- Ion Pacepa, *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism* (Independently Published, 2013).
- Peter Pomerantsev, *This is Not Propaganda: Adventures in the War Against Reality* (Public Affairs, 2019).

- NATO StratCom Centre of Excellence, https://stratcomcoe.org/.
- Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Profile Books, 2021).
- Viginum, https://www.sgdsn.gouv.fr/.

Social and political NSAs

- Andis Kudors, *Russia and Latvia: A Case of Sharp Power*, (Routledge, 2024).
- Anton Barbashin and Alexander Graef, 'Thinking Foreign Policy in Russia: Think Tanks and Grand Narratives', Eurasia Center Report (Atlantic Council, November 2019), https://www.atlanticcouncil.org/wp-content/uploads/2019/11/Thinking-Foreign-Policy-in-Russia_-Think-Tanks-and-Grand-Narratives-Atlantic-Council-11.12.19.pdf.
- Fredrik Wesslau, 'Putin's friends in Europe', European Council on Foreign Relations, 19 October 2016, https://ecfr.eu/article/commentary_putins_friends_in_europe7153/.
- Joshua P. Mulford, 'Non-State Actors in the Russo-Ukrainian War', *Connections QJ* 15, no. 2 (2016): 89–107.
- Orysia Lutsevych, 'Agents of the Russian World Proxy Groups in the Contested Neighbourhood', Russia and Eurasia Programme (Chatham House, April 2016), https://www.chathamhouse.org/sites/default/files/publications/research/2016–04–14-agents-russian-world-lutsevych.pdf.
- Raphaël Kergueno, 'From Russia with Lobbying', Transparency International EU, 5 July 2017, https://transparency.eu/russialobbying/.
- Susi Dennison and Dina Pardijs, 'The world according to Europe's insurgent parties: Putin, migration and people power', ECFR Flash Scorecard (European Council on Foreign Relations, June 2016), https://ecfr.eu/wp-content/uploads/ECFR_181_-_THE_WORLD_ACCORDING_TO_EUROPES_INSURGENT_PARTIES_NEW.pdf.

Economic and financial NSAs

- David Lewis and Tena Prelec, 'New Dynamics in Illicit Finance and Russian Foreign Policy', SOC ACE Research Paper 17 (University of Birmingham, August 2023), https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/64d9c7660051ed7fd7e34902/1731067227329/SOCACE-RP17-NewDynamics-Aug23.pdf.
- Catherine Owen, Tena Prelec and Tom Mayne, 'The Illicit Financialisation of Russian Foreign Policy, SOC ACE Research Paper 3, (University of Birmingham, May 2022) https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/6481ed0061707e40ea865aad/1686236417031/SOCACE-RP03-Illicit_Financialisation-Jun23.pdf.

- Greg Rosalsky, 'How Putin Conquered Russia's Oligarchy', Planet Money, 29 March 2022, https://www.npr.org/sections/money/2022/03/29/1088886554/how-putin-conquered-russias-oligarchy.
- Justyna Gudzowska, Eliza Lockhart and Tom Keatinge, 'Disabling the Enablers of Sanctions Circumvention', RUSI Policy Brief (RUSI, May 2024), https://www.rusi.org/explore-our-research/publications/policy-briefs/disabling-enablers-sanctions-circumvention.
- Olivia Allison and Tom Keatinge, 'Strengthening the Financial Frontline on Russian Trade Sanctions', RUSI Policy Brief (RUSI, March 2025), https://www.rusi.org/explore-our-research/publications/policy-briefs/strengthening-financial-frontline-russian-trade-sanctions.
- Matthew Redhead, 'Old Wine, New Bottles? The Challenge of State Threats', SOC ACE Research Paper 32, (University of Birmingham, January 2025), https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/67852e69ff4ff4079a9c3000/1736781420568/SOCACE-RP32-OldWineNewBottles_final.pdf.
- Olivia Allison et al., 'Wagner's Business Model in Syria and Africa: Profit and Patronage', RUSI Occasional Paper, (RUSI, 6 February 2025), https://www.rusi.org/explore-our-research/publications/occasional-papers/wagners-business-model-syria-and-africa-profit-and-patronage.
- Spencer Woodman, 'How a network of enablers have helped Russia's oligarchs hide their wealth abroad', International Consortium of Investigative Journalists, 2 March 2022, https://www.icij.org/investigations/russia-archive/how-a-network-of-enablers-have-helped-russias-oligarchs-hide-their-wealth-abroad/.
- Tom Keatinge, 'Developing Bad Habits: What Russia Might Learn From Iran's Sanctions Evasion', RUSI Occasional Paper, (RUSI, June 2023), https://static.rusi.org/developing-bad-habits-what-russia-might-learn-from-irans-sanctions-evasion.pdf.

Appendices

TABLE A1. PMC archetypes[396]

South African model	American model	Wagner model
• Closely aligned with traditional mercenary operations. • Exemplified by companies such as Executive Outcomes and Sandline International.	• Characterised by "military entrepreneurship". • They may engage in combat, but this is not their *raison d'être*. • Their primary function is to provide security services and non-combat operational support. • Exemplified by companies such as Blackwater, DynCorp, and the British company Aegis Defence Services.	• A paramilitary, parastatal, mafia-type organisation that merges state-directed violence with organised crime. • While not all Russian PMCs fit this mould, Wagner became the prototype most aligned with the Kremlin's preference for deniable coercive force projection.

Context: Broadly speaking, there are three PMC archetypes, presented in the table above: the South African mercenary model, the American model characterised by military entrepreneurship, and the Wagner Group hybrid model, which blends parastatal, paramilitary, and criminal elements.

396 Adapted from 'The Business of War – Growing Risks from Private Military Companies', Council of the European Union, Analysis and Research Team – Research Paper, 31 August 2023, https://www.consilium.europa.eu/media/66700/private-military-companies-final-31-august.pdf.

TABLE A2. Evolution of the global hacktivist environment

Digital utopia era (1985–2005)	**Anti-establishment era (2006–2013)**	**Establishment era (2014–present)**
• Primarily composed of ethical hackers who envisaged a better internet, promoted free information and digital rights, and sought to draw attention to IT security issues.	• Hacktivists primarily targeted governments and large corporations without any clear ideological alignment. • Groups were decentralised and lacked a clear structure and hierarchy.	• Hacktivists moved away from anti-government sentiment and began openly aligning with certain nation-states, particularly Russia and Iran.
Example: Chaos Computer Club in Germany and Cult of the Dead Cow in the US.	**Example:** Anonymous and LulzSec	**Example:** Pro-Russian hacktivist group Killnet and pro-Ukrainian IT Army of Ukraine.

Context: The global hacktivist community has evolved significantly since the early days of the internet. What began as an independent movement driven by pure idealism has become a valuable tool for states seeking to advance their geopolitical ambitions.

397 Adapted from Orange Cyberdefense's 'Security Navigator 2025'. https://www.orangecyberdefense.com/uk/security-navigator.

TABLE A3. Evolution of the Russian oligarchy

First wave	Second wave
• The first group of oligarchs emerged after the collapse of the Soviet Union in the 1990s and gained immense economic power by purchasing formerly state-owned companies. • These businessmen used their economic influence to exert significant political pressure on the Yeltsin government.	• The second group emerged after Putin became President of Russia in 2000. • Putin facilitated the enrichment of a second generation of oligarchs through lucrative state contracts.[398] • This system has allowed Putin to cultivate a loyal circle of elites whose vast wealth is directly tied to their relationship with the Kremlin. • By 2021, approximately 500 oligarchs controlled 40% of Russia's entire household wealth.[399]

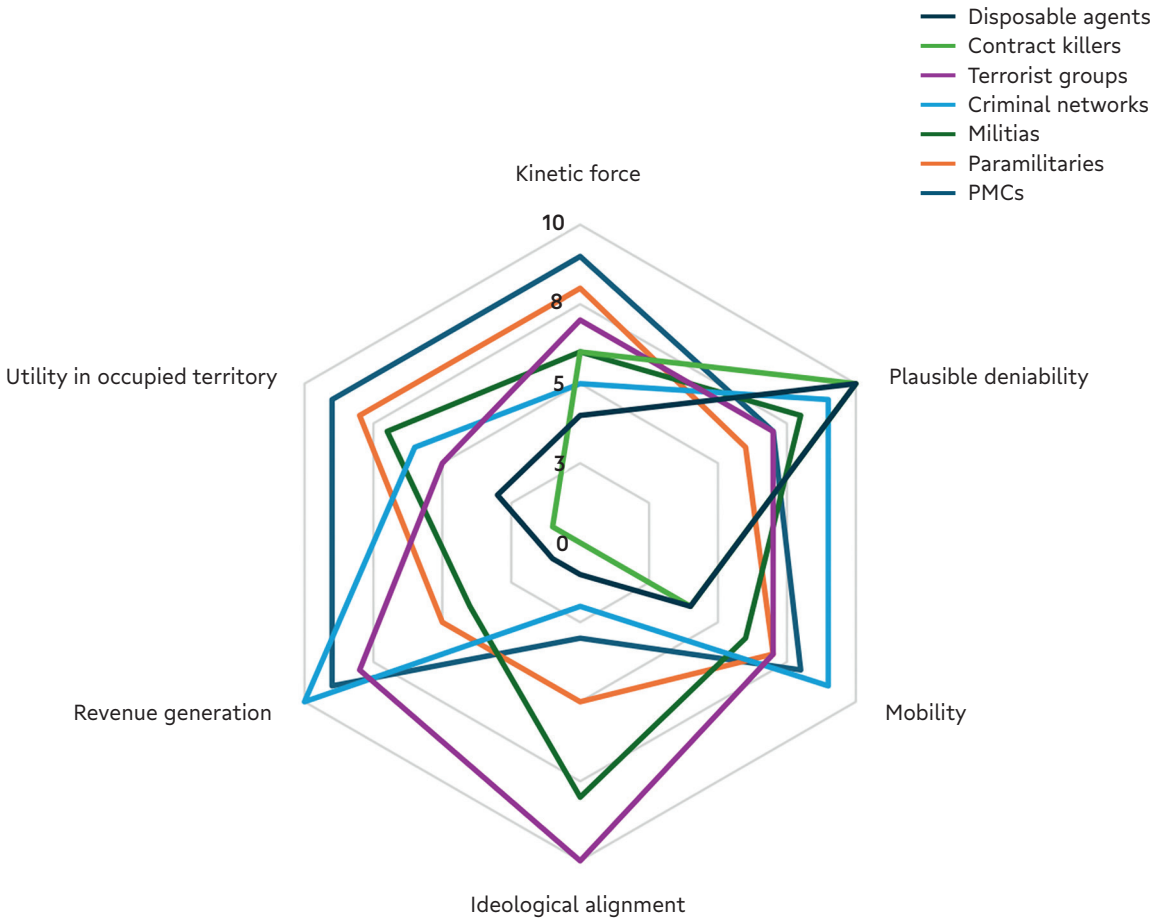
Context: After the collapse of the Soviet Union, the Yeltsin government embarked on a programme of privatisation, selling off key assets in the energy, metallurgical, mining, shipping, and financial sectors through the infamous "loans-for-shares" scheme. Under this scheme, shares in state-owned companies were offered in exchange for loans to secure the Russian federal budget. When the Russian government under Yeltsin deliberately defaulted on these loans in 1996, the shares were auctioned off to the oligarchs for a fraction of their value. While this enabled Yeltsin to secure funds for his re-election as president, it concentrated economic power in the hands of a small group of oligarchs.[400]

398 Private firms in critical sectors such as defence, infrastructure, construction, and healthcare charge the government far above market rates and share the profits through kickbacks to complicit state officials. See Stanislav Markus, 'Oligarchs and Corruption in Putin's Russia: Of Sand Castles and Geopolitical Volunteering', *Georgetown Journal of International Affairs* (Summer/Fall 2017), https://ssrn.com/abstract=3003409.

399 'BTI 2024 Country Report – Russia', Country Report, (Bertelsmann Stiftung, 2024), https://bti-project.org/fileadmin/api/content/en/downloads/reports/country_report_2024_RUS.pdf, 18.

400 See Marshall Goldman, *The Piratization of Russia: Russian Reform Goes Awry* (Routledge, 2003); Harry Atkins, 'How Did Russia's Oligarchs Get Rich From the Fall of the Soviet Union?', *HistoryHit*, 8 April 2023, https://www.historyhit.com/how-did-russias-oligarchs-get-rich/; Brian Whitmore, 'Russia: The End of Loans-For-Shares', *Radio Free Europe/Radio Liberty*, 29 September 2005, https://www.rferl.org/a/1061761.html.

FIGURE A1. ANSAs by operational domain

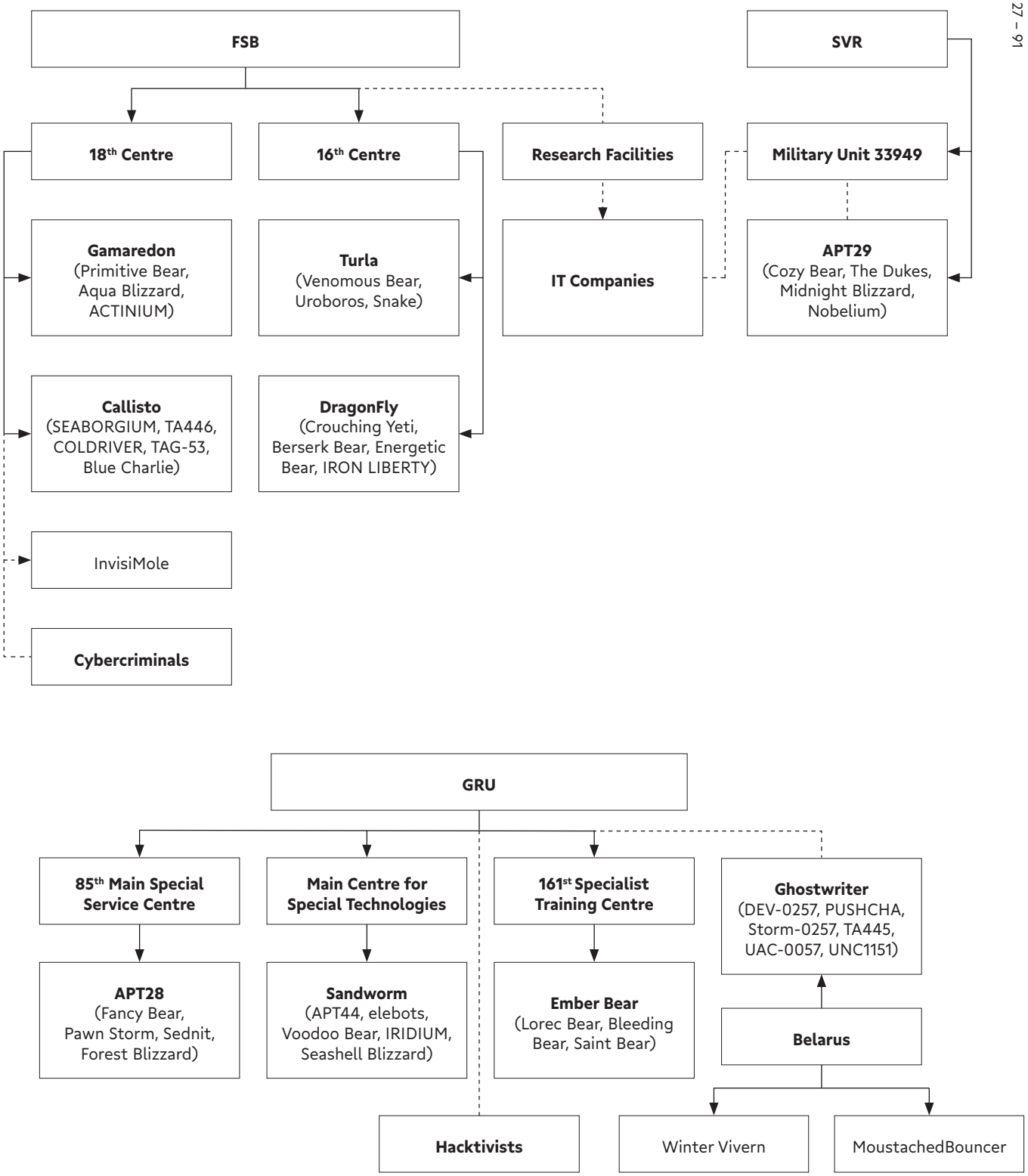


Context: This analysis was based on qualitative comparative analysis and interpretive synthesis to help the reader visualise the strategic role of different ANSA sub-categories. It is not based on quantitative data.

The typology and scoring were conducted across six operational domains. Scores were assigned based on the perceived degree of institutional embedding, visibility, and functional use by Russia. For instance, PMCs received a score of 9 in Kinetic force due to Wagner's record of combat operations and direct action. TCNs scored 10 in Revenue generation but lower in Ideological alignment due to opportunism. Contract killers scored high on Plausible deniability , but low on Mobility and Utility in occupied territory. The radar chart is not based on a quantitative dataset but rather on an interpretive framework designed to provide a visual aid that compares the strategic role of different ANSA sub-categories.

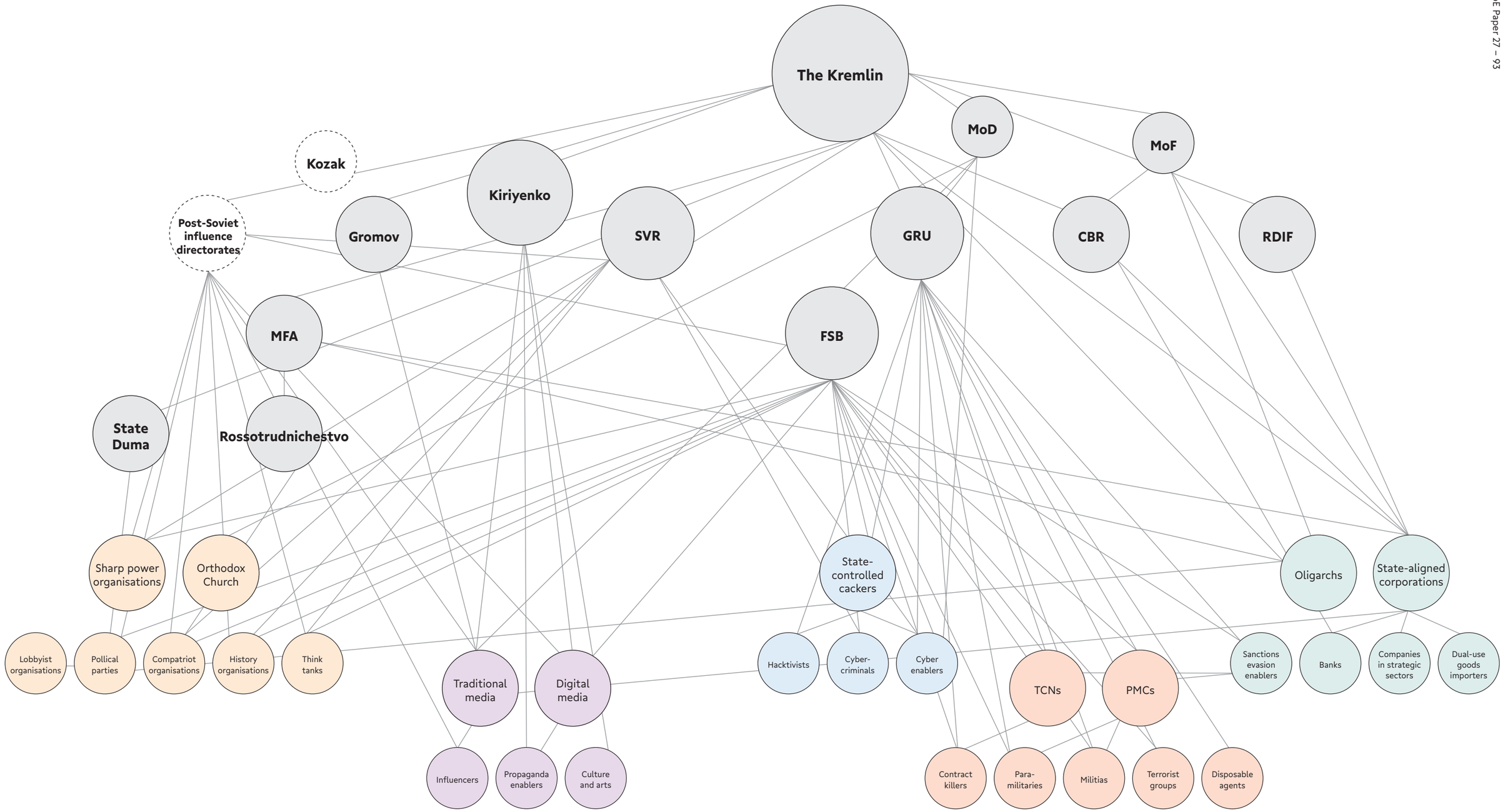
- **Kinetic force:** Capacity for armed violence.
- **Plausible deniability:** Ability to shield the Kremlin from direct blame.
- **Mobility:** Operational flexibility across regions and missions.
- **Ideological alignment:** Degree of ideological overlap with Kremlin narratives.
- **Revenue generation:** Ability to produce or manage funds (licit or illicit).
- **Utility in occupied territory:** Effectiveness in maintaining control or exerting influence.

FIGURE A2. Russian cyber ecosystem



Context: The information presented in the diagram is based on publicly available reporting and leaked documents. It should be viewed as an indicative representation rather than a definitive account of the Russian cyber ecosystem, as the underlying data are difficult to verify.

FIGURE A3. Links between various categories of NSAs and Russian state institutions as of spring 2025



Context: This figure visualises the state institutions responsible for or connected to the various NSAs discussed in the report. The links between these state institutions and NSAs are based on publicly available sources used in the preparation of the report. The figure does not claim to provide a definitive overview of the NSA ecosystem in Russia but reflects the situation as of spring 2025. It excludes subsequent developments, such as Dmitry Kozak's dismissal and the reformation of the directorates for influencing post-Soviet states in late August/September 2025.

Authors

Eginhards Volāns is a senior analyst at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). He currently focuses on the role of non-state actors in hybrid threats, with a particular emphasis on the use of proxies in Russian hybrid threat operations. He also co-leads Hybrid CoE's hybrid threat monitoring group, which tracks major incidents and analyzes the evolving hybrid threat environment.

Dr **Vladimir Rauta** is the Head of the Department of Politics and International Relations and the Director of the Centre for Global Security and Governance at the University of Reading, United Kingdom.

Magda Long is a specialist in intelligence, covert action, and hybrid threats posed by states and armed non-state actors, with over two decades of combined professional and academic experience in international security. She is a consultant and visiting research fellow at several leading academic institutions in the United States and the United Kingdom. Dr Long is the lead editor and a contributing author of Covert Action: National Approaches to Unacknowledged Intervention, a groundbreaking volume examining covert practices of 20 nations. She holds a PhD in War Studies from King's College London.

Andis Kudors (PhD candidate) was a visiting scholar at the Institute for European, Russian and Eurasian Studies, the Elliott School of International Affairs (George Washington University) in 2021–2022. He is a 1996 graduate of the International Law and Economics Program at the University of Latvia Institute of International Affairs. From 2005 until 2011, he studied at the University of Latvia, specializing in Russian foreign policy, and earned a BA and then an MA in political science. In 2006–2019, Mr Kudors was the Executive Director of the Centre for East European Policy Studies. His research interests include national security, soft power, sharp power, propaganda, disinformation, and informational warfare. Andis Kudors is an author of many analytical articles about Russian foreign policy and Latvian security. He has been a Fulbright scholar at the Kennan Institute (Woodrow Wilson Center) in Washington DC (2014–2015). In 2021, Andis Kudors was appointed Commander of The Cross of Recognition by the President of the Republic of Latvia, Egils Levits, for his contribution to the research of Latvian national security.

Agata Kleczkowska is an Assistant Professor at the Institute of Law Studies of the Polish Academy of Sciences. Her area of expertise covers public international law, including especially the questions of the use of force, hybrid threats, the status of non-state actors, and international organisations. Among other functions, she is a Managing Editor of the Contemporary Central & East European Law journal, a Co-Editor of the Digest of State Practice of the Journal on the Use of Force and International Law, and a member of the NATO STO Research Task Group on the Ethical and Legal Challenges of Cognitive Warfare.

Eliza Lockhart is a Research Fellow at the Centre for Finance and Security (CFS) at the Royal United Services Institute, the UK's leading defence and security think tank. Her work examines matters at the intersection of law, finance and security, with a focus on hybrid threats and economic security. Prior to joining CFS, she was a lawyer at a top-tier global law firm. She holds a Master of Law and an MPhil in Public Policy, both with Distinction from the University of Cambridge.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats