ZINC NETWORK

ISET POLICY INSTITUTE
International school of economics at TSU

A Study on the Risks Associated with Russian Business Ownership in Georgia

SEPTEMBER 2023

The report was prepared by ISET Policy Institute with the support of the USAID Information Integrity Program.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The provided study aims to investigate potential risks associated with Russian business ownership in various sectors of the Georgian economy. The research is grounded in sectoral analysis conducted by the Institute for the Development of Freedom of Information (IDFI). In particular, we assess potential risks linked to Russian business ownership across eight industries: electricity, oil and natural gas, communications, mining and mineral waters, tourism, banking, construction, and transportation.

The sectoral assessment of Russian business ownership in the examined industries reveals concerning signs of ownership concentration, particularly in the electricity sector, followed by oil and natural gas, communications, and mining and mineral waters industries. In terms of tourism, banking, construction, and transportation, we find low to non-existent ownership-related influence.

To identify the specific risks associated with Russian business ownership, this study draws upon a comprehensive literature review and conducted expert interviews. The study places Russia within the context of a global threat actor and examines the exploitation of private business ownership by hostile state actors as a hybrid threat. We pay special emphasis on the significance of the concentration of Russian business ownership in Georgian critical industries (that potentially involve Critical Infrastructure (CI)), such as electricity, communications, and sea port - prompting considerable security implications.

Specifically, the study identifies six distinct risks associated with Russian citizens or companies owning businesses in Georgia. Firstly, we argue that ownership could grant Russia increased **political influence** over Georgia, given the interconnected interests of Russian political and business elites. Secondly, we highlight the risk of **exporting corruption** (e.g., tax evasion, money laundering, "revolving door" incidents, exploiting public procurement systems, etc.) as a significant concern, given the history of corrupt practices by Russian businesses in both the Georgian and neighboring contexts.

Thirdly, our analysis demonstrates that **economic dependency** presents yet another risk, potentially exposing Georgia to economic manipulation, including price distortions. Moreover, **espionage**—be it commercial, political, or involving personal information—is viewed as an additional risk tied to Russian ownership, drawing from empirical evidence that indicates connections between Russian business operators (e.g., Yandex Go) and Russian intelligence agencies.

Furthermore, we identify **sabotage** as another potential risk that could materialize through the conduit of Russian business ownership in Georgia. Lastly, the study underscores the risk of **sanctions and sanctions evasion**, considering the existing sanction regimes that target Russia and Russia-affiliated businesses on a global scale.

Considering judgment of our interviewed experts, the study explores the severity levels associated with the identified risks. This risk assessment exercise shows that each of the identified risks carries a high severity level. However, it is significant to allocate special attention to the risks of political influence, the export of corruption, and the potential for sanctions and sanctions evasion. Furthermore, the ownership factor notably intensifies the severity level of the risk tied to economic dependency.

As a final step of the research, we explore potential strategies to mitigate adverse impacts of identified risks. Considering international practices, we pay specific emphasis to introducing Foreign Direct Investment (FDI) screening mechanism as the most effective tool to alleviate potential harms stemming from those foreign investments in business ownerships, which have harmful security implications.

The analysis issues three recommendations:

1. **Study the Potential Impact of Adopting a Foreign Direct Investment (FDI) Screening Mechanism**

   Currently, a substantial proportion of countries worldwide, accounting for at least one-third, have already implemented some form of investment review procedure. Nonetheless, it is important to note that diverse manifestations of investment screening procedures exist. These include reviews limited to Critical Infrastructure (CI), mechanisms designed to selectively examine inward FDIs originating from malign state actors of a certain, pre-defined volume, or investment review procedures with retrospective authority (e.g. for Georgia, it might be suitable to adopt an *ex-ante* screening mechanism of Russian-originated investments in critical sectors, through which an owner acquires at least 10% of shareholding rights).

   Further, while FDI review mechanisms hold the potential for significant positive outcomes, they may also bring some notable economic harms. In light of this, the study advocates for a comprehensive assessment of the appropriateness and potential consequences of introducing an FDI screening mechanism within the context of Georgia.

2. **Consider Russian Ownership-related Threats in National Conceptual Documents of Security**

   In the process of designing the FDI screening mechanism, it is crucial to base the scope of this instrument on a comprehensive recognition of the risks associated with Russia's business ownership in Georgia, as outlined in national foundational security documents such as the National Security Concept or the National Threats Assessment Document. At present, the National Security Concept includes only a general acknowledgment of Russia's military and hybrid threats, while the availability of the National Threats Assessment Document remains limited.

However, should the FDI screening mechanism potentially adopt a targeted approach to inward FDIs within critical sectors originating from Russia, it becomes imperative that the rationale for such a tool is rooted in the principles given within the nation's fundamental security documents.

3. **Foster the Adoption of Critical Infrastructure Reform through an Inclusive Policy Process**

Another significant step that has to be taken in order to move forward to operationalize recommendations regarding implementing an FDI screening mechanism, will be to foster the process around adopting Critical Infrastructure reform in Georgia. Fostering adoption of this reform will be significant to have a nationwide agreement regarding the legal foundations for identifying and protecting Georgia's critical infrastructure.

Significantly, Georgia is in the process of adopting Critical Infrastructure reform. Thus, implementing this reform will practically translate into operationalization of our main recommendation to mindfully consider the establishment of some form of investment review procedure in the country.

INTRODUCTION

Russia wields substantial leverage over Georgia, particularly considering its military occupation of 20% of the country's internationally recognized territories – Abkhazia and South Ossetia. Nevertheless, beyond this military presence, Georgia faces a range of other unconventional and hybrid threats from Russia. One such strategic hybrid tactic involves exploiting economic dependency to hinder resilient development in Georgia.

The expanding economic influence that Russia exerts within Georgia gives rise to multiple forms of threat, notably those within the concepts of "economic capture" and "political capture," as identified by Conley, Mina, Stefanov, and Vladimirov (2016). As such, given Georgia's lack of robust institutional checks to effectively counteract these influences, the potential consequences of such threats might evolve into the elevated risk of "state capture".[1]

Russia's present economic footprint in Georgia is determined through various components, including its trade relationship, the reliance on money remittances originating from Russia, boosted economic activity facilitated via the influx of Russian migrants, and, with other determining factors, through private business ownership, either by Russian companies or its citizens.

This study specifically observes the latter component of Russia's economic footprint – private business ownership within the Georgian economy. Furthermore, the study considers the specific risks that might materialize due to Russian business ownership. The core findings of this research are based on a sectoral overview of Russian business ownership conducted by the Institute for Development of Freedom of Information (IDFI). Thus, the given analysis solely covers those economic sectors which have already been researched by the IDFI.[2]

Through a literature review and qualitative expert interviews, this study places Russia within the context of global threats and it regards this hostile state actors' utilization of private business ownership as a hybrid threat. As a result, this research pinpoints and evaluates six distinct risks linked with the Russian presence in the Georgian economy via private business ownership. Table 1 briefly summarizes the identified risks and the interrelated scopes:

[1] In their trilogy, *Kremlin Playbook*, Conley, Mina, Stefanov, and Vladimirov (2016) emphasize that, in the national contexts of Eastern and Central Europe, the growing Russian economic footprint created risks of political and economic capture, which then further materialized into the risk of state capture (Conley, Mina, Stefanov, & Vladimirov, 2016, p. 11).

[2] The IDFI sectoral overview covers the following spheres: Electricity; Oil and Gas; Communications; Mining and Mineral Waters; Tourism; Construction; Banking; and Transportation.

Table 1: *Georgia-specific risks of Russian business ownership*

RISK	SCOPE OF RISK
Political Influence	The interests of the Russian business elite are closely intertwined with those of the Russian political elite. There is thus a likelihood that Russia seeks to exert influence over Georgian politics and its policy-making through ownership channels.
Exporting Corruption	Russian ownership in Georgian business has the potential to foster corrupt practices, which may manifest through incidents such as the 'revolving door,' tax evasion, or exploitation of the public procurement system
Economic Dependency and Manipulation	A significant concentration of Russian ownership within any sector of the Georgian economy gives rise to the risk of "sphere capture," whereby Russia could potentially disrupt the function of a "captured sector" by manipulating economic instruments, such as prices.
Espionage	Russian ownership could potentially serve as a channel for transferring sensitive information from Georgia to Russian intelligence agencies. This information might encompass company-related data, personal details, and political secrets, among other sensitive material.
Sabotage	Russian business ownership offers further potential to facilitate potential acts of sabotage, including cyber-sabotage, aimed at causing either permanent or temporary incapacitation of specific assets or networks.
Sanctions and Sanction Evasion	Companies owned by Russian entities could find themselves targeted by sanction regimes due to their ownership. These companies might also evolve into havens for evading sanctions. The shifting of ownership in response to sanctions could add to the existing lack of transparency concerning the management of such entities.

An evaluation of the identified risks highlights the severity associated with each factor. However, particular attention should be directed towards the risk of political influence, the export of corruption, and the potential for sanctions and sanction evasion. Moreover, the ownership factor significantly amplifies the severity level of risks related to economic dependency and manipulation.

In addition to identifying and assessing risks, this study delves into the topic of risk mitigation measures, with particular emphasis on Foreign Direct Investment (FDI) screening mechanisms as a tool for effectively managing ownership that poses security concerns. Given the diverse range of FDI screening mechanisms available and the potential economic impacts of each, we recommend a thorough examination into the efficiency and desirability of implementing this policy change.

Therefore, to operationalize this recommendation, we believe it crucial to incorporate an overview of Russian ownership-related risks within the national conceptual documents on security. Additionally, fostering the adoption of Georgia's critical infrastructural reform is considered critical in realizing this approach.

The subsequent sections of the report present a detailed study of the risks associated with Russian private ownership in Georgian businesses. It commences with a review of IDFI's sectoral research findings concerning the extent of Russian ownership. Thereafter, the report reviews the relevant literature from two perspectives: a) Russia as a threat actor and b) foreign ownership as a hybrid threat. Notably, special attention is devoted to highlighting the vulnerabilities of critical infrastructure related to foreign ownership.

Building on the insights gathered from the literature reviews and expert interviews, the report identifies and assesses specific risks relevant to Georgia within the framework of Russian private business ownership. Concluding the analysis, the study presents a range of risk mitigation measures and offers key recommendations.

SECTORAL OVERVIEW OF RUSSIAN OWNERSHIP IN GEORGIAN BUSINESSES

Russian ownership has been long present in the history of modern Georgia. Each elected government has to some extent welcomed Russian capital into the country, including within critical sectors, such as energy and communications. Critically, a detailed study of Russian capital accumulation and linkages in Georgian businesses has been conducted by the Institute for Development of Freedom of Information (IDFI). This research has been communicated to the public in several waves; first in 2015, and then consecutively in 2022 and 2023.

At this stage, the IDFI has investigated Russian capital accumulation over several sectors, in particular: electricity; oil and gas; communications; banking; mining and mineral waters; construction; tourism; and transportation. Based on these conclusions, the Russian business linkages of utmost concern are within the electricity sector, followed by the sectors of oil and gas, communications, and mining and mineral waters. As the research has revealed, there is currently no notable or concerning business linkage present in the banking, construction, tourism, or transportation sectors. Nevertheless, dependency on Russian capital is growing amidst the war in Ukraine, and due to the intensified influx of Russian migrants in Georgia. The section below briefly summarizes the main IDFI research findings relating to Russian business ownership in Georgia.

ELECTRICITY

According to the IDFI, a significant position on the Georgian energy market is held by the Russian company Inter RAO. With its ownership of the Khramhesi 1 and Khramhesi 2 hydropower plants (HPPs)[3], the company might have its control over significant part of Georgia's total electricity consumption. Inter RAO also holds a notable stake in Telasi JSC (Telmico from 2020) – the only electricity supplier for the 697 400 subscribers in the Georgian capital; in total, Tbilisi consumes 20% of the country's overall electricity, amounting to 3 billion kWh (Institute for Development of Freedom of Information (IDFI), 2023, p. 18).

A 75.11% stake of Telasi JSC is held by Silk Road Holding B.V., which is entirely owned by Inter RAO, which, in turn, is owned and controlled by Russian state companies (including Rosneftegaz, Inter RAO Capital, and Rosetti FGC UES). A large part of the remaining 24.53% Telasi shares are held by the Best Energy Group company, owned by the businessmen Khvicha Makatsaria; who in May 2022, acquired 100% of Veon Georgia (Beeline), a company that has been associated with Mikhail Fridman, the sanctioned Russian businessman. Moreover, Khramhesi 1 and Khramhesi 2

[3] In 2008, memorandum was signed between the Georgian Ministry of Energy and Inter RAO, which led to the company's participation in the joint management of Enguri HPP (Institute for Development of Freedom of Information (IDFI), 2023, p. 19). Specific details regarding the management practices of Enguri HPP have remained undisclosed to the public so far. It is however important that the Georgian state retains 100% ownership of the company and senior staff at Enguri HPP have denied any involvement of 'Inter RAO' in the company's management.

are both owned by Gardabani Holding B.V., which is also directly owned by Inter RAO (Institute for Development of Freedom of Information (IDFI), 2023, p. 18).

There is another company related to Russian "Inter RAO". An intermediary Lux Energy Trading LLC, formerly known as Inter RAO Georgia LLC, registered "as a participant in wholesale trade as an exporter, importer and wholesale supplier of electricity" (Transparency International Georgia, 2023). The company is involved in electricity trading, namely importing electricity to Georgia from Russia (Transparency International Georgia, 2023).

Russian linkages have moreover been traced to energy projects that are currently underway, those which are projected to generate in total 751 million kWh of electricity. Specifically, Mtkvari Energy LLC is constructing the Mtkvari HPP, with an estimated annual electricity production of 251 mln. kWh, while Dariali Energy JSC manages the Dariali HPP project in Kazbegi, with an annual electricity output of 500 mln. kWh. The Dariali HPP project further envisages connecting the power plant to the national grid via a 100-kW transmission line (Institute for Development of Freedom of Information (IDFI), 2023, pp. 21-22).

Notably, Mtkvari Energy is owned by Mtkvari Holding LLC, with GCF Partners LLC managing the company's shares. GCF Partners equally act as a managing company for Georgia's co-investment fund, and it is solely owned by Giorgi Bachiashvili, who holds dual Georgian and Russian citizenship. Additionally, the current director of energy projects at Mtkvari Holding sits on the supervisory board of Georgian State Electricity System JSC, which is "the sole operator of Georgia's electricity transmission system, responsible for transmitting and dispatching electricity to distribution companies and directly to consumers, sourced from hydro, thermal, and wind power plants (Institute for Development of Freedom of Information (IDFI), 2023, p. 21)."

Regarding Dariali Energy JSC, 44.27% of company shares are held by Energia LLC, of which 70% of shares are held by Russian citizen, Mevludi Bliadze, while 30% belongs to Feri LLC. Together, Mevludi Bliadze and Feri LLC own the Shildahesi HP station, which generated 0.1% of total Georgian electricity production in 2021 (Institute for Development of Freedom of Information (IDFI), 2023, p. 22).

Lastly, Pshavi Hydro LLC owns the small Skurdidi HPP, with a capacity of 1.33 megawatts. The company is controlled by two shareholders, Rauli Kurdadze (87%) and Zviad Gugava (13%), both of whom hold dual Russian and Georgian citizenship (Institute for Development of Freedom of Information (IDFI), 2023, p. 22).

Besides electricity supply, generation, and trade, Russian linkages can also be identified within other significant fields of the Georgian energy sector. Specifically, Sakrusenergo JSC, which owns and manages important power transmission lines (including those from which Georgia receives Russian electricity), is owned jointly by the Georgian state (50%) and the Russian Federal Grid Company of United Energy System (Institute for Development of Freedom of Information (IDFI), 2023, p. 20).

Significantly, Sakrusenergo JSC already owns or has permission to build crucial transmission lines, such as the 500 KV HV electric transmission lines for Kavkasioni, Kartli 1, Kartli 2, Imereti, Imereti 2, Assureti, Stepantsminda-Mozdok, Mukhrani, Mukhrani Valley, and Marneuli-Airum; the Gardabani 330 KV HV electric transmission line; and the Adjara 220 KV HV transmission line. Through these lines, Sakrusenergo operates both internal systems and it connects Georgia with Russia, Azerbaijan, and with Turkey (Institute for Development of Freedom of Information (IDFI), 2023, p. 20).

An assessment of Russian business linkages in the Georgian electricity sector raises particular concerns regarding its secure and resilient operations, especially in consideration of the essential service it provides. Such concerns are further heightened given that Russian business ownership in the sector is present simultaneously within different streams of electricity generation, supply, transmission, and trade.

OIL AND GAS

As per the IDFI report, there is scarce evidence of Russian ownership in operators within the Georgian oil market beyond Lukoil and Gulf, which are included in the top five retail operators and share 59% of the respective market in Georgia. In contrast, there has been no detectable sign of Russian business ownership in the natural gas sector (Institute for Development of Freedom of Information (IDFI), 2023, p. 24).

Lukoil Georgia is owned by the Russian Lukoil Public JSC, which was sanctioned by the USA in January 2022, thereby limiting the company's oil projects. According to company data, it operates 57 stations in Georgia, 21 of which are in Tbilisi. The company also actively participates in Georgian public tenders, where the total value of contracts signed between state agencies and Lukoil Georgia constitutes over 200 mln. GEL (Institute for Development of Freedom of Information (IDFI), 2023, pp. 24-25).

Lukoil has moreover been associated with the former prosecutor of Georgia, Otar Partskhaladze, who served as their deputy director in 2017. Previous journalistic investigations have also revealed that potentially corrupt oil transportation schemes directly involved Otar Partskhaladze and Lukoil (Institute for Development of Freedom of Information (IDFI), 2023, p. 25).

Another major player on the Georgian oil market is Petrokas Energy Georgia, which has associations with the Russian company Rosneft and with Davit Iakobashvili, a Georgian businessman. Notably, Petrokas is a significant stakeholder on the Georgian oil market and it trades oil products. It also holds shares in several oil companies, such as Channel Energy (Poti) Limited (the Poti oil terminal), San Petrolium Georgia (a chain of Gulf gas stations), and Gulf Aviation. Channel Energy (Poti) Limited owns a 32.67% share in the Poti oil terminal, while the remaining shareholders are registered in the Virgin Islands. Moreover, Gulf Aviation supplies the international airports in Tbilisi, Kutaisi, and Batumi, and its fuel supplies are consumed by several major airlines

operating in Georgia. Lastly, San Petrolium Georgia is included within the top five players on the local oil market (Institute for Development of Freedom of Information (IDFI), 2023, p. 25).

Until 2022, a 49% stake of Petrokas Energy Georgia belonged to Rosneft. In May 2022, following sanction packages related to the Russian war in Ukraine, Vano Nakaidze, CEO of Petrokas, acquired shares from the Russian Rosneft, removing notable Russian presence from the company. A little later in 2022, however, War and Sanctions, a Ukrainian platform, communicated that the parent company (Petrokas Energy International Limited) and its founder (David Iakobashvili) were also linked with the Russian regime (Institute for Development of Freedom of Information (IDFI), 2023, pp. 25-26).

Considering the ownership structure of Lukoil Georgia, alongside the previous Russian associations with Petrokas Energy Georgia, one can thus trace notable ownership-related influence within the Georgian oil and gas sector.

COMMUNICATIONS

Russian ownership in the communications sector has been connected to the cellular communication company Veon Georgia and to interests in the sector via Fridon Injia's family. Injia is a Georgian political figure with outspoken anti-western sentiments who expressly advocates for closer ties with Russia. Injia's family members (his son and spouse) have dual citizenship with both Russia and Georgia (Institute for Development of Freedom of Information (IDFI), 2023, pp. 10-11).

Veon Georgia, a cellular communication company, also known under the name of the mobile operator Beeline, is currently owned by Khvicha Makatsaria, a Georgian businessman, who purchased 100% of its shares in 2022. Before which, one co-owner in Beeline Georgia was the sanctioned Russian businessmen Mikhail Fridman (Institute for Development of Freedom of Information (IDFI), 2023, p. 1). However, as of now, no clear Russian ties have been found in Veon Georgia.

Beyond Veon Georgia, significant interests in the communications market are concentrated in the hands of Fridon Injia and his family. According to the IDFI, "Fridon Injia controls 25.19% share of the landline telephone market and 6.2% of the fixed internet connection market in Georgia." Namely, Injia's companies in the communications sector include: Akhali Kselebi, System Net, CGC, and Fopnet (Institute for Development of Freedom of Information (IDFI), 2023, pp. 10-11).

Fopnet provides telecommunication services through long-distance channels from Tbilisi to large Georgian cities, and from Tbilisi to Russia, the CIS, Europe, and to Asia. Moreover, Fopnet owns the Georgia-Russia fiber optic cable. The company additionally has a partnership with the Russian Vestelcom, a subsidiary of the communications company Rostelcom (Institute for Development of Freedom of Information (IDFI), 2023, p. 11).

Besides the aforementioned connections, Russian ownership has also been detected in the broadcasting company R.B.G., which transmits translations of the Russian Public Broadcaster (ORT). The owners of this company are Irakli Adamia (10%), a Georgian citizen, and the Russian, Olga Milieva (90%) (Institute for Development of Freedom of Information (IDFI), 2023, pp. 11-12).

Considering the interests of Injia's family and the previous Russian connections of Veon Georgia, an assessment of the Georgian communications sector raises moderate concerns regarding the potential risks and threats that might arise from Russian ownership

MINING AND MINERAL WATERS

According to the IDFI, there are 3,069 active companies holding licenses and operating in the mining and mineral waters sector in Georgia. However, there are seven core companies that have distinct ties with Russian businesses and citizens, including: Rich Metals Group (RMG), Capital Group LTD, Mega Holding (Tbilcement Group), Sairme Mineral Water, IDS Borjomi, Gurzvinprom, and Mixor (Institute for Development of Freedom of Information (IDFI), 2023, pp. 13-17). Table 2 below summarizes the general information regarding these companies and their connections with Russia.

Table 2: *Companies with Russian connections in the mining and mineral waters sector (Institute for Development of Freedom of Information (IDFI), 2023, pp. 13-17)*

Company Information	Russian Connection
RMG (Rich Metals Group) holds a gold mining license for 2014-2042 and is connected with the removal of the Sakdrisi monument. It also holds an additional six licenses for mining other minerals and mineral waters. Another company affiliated with RMG is RMG Auramine, which holds licenses for gold and freshwater. As of April 2015, the company's actions have been associated with more than 30 mln. GEL in damage to the environment.	Rich Metals Group is owned by RMG Copper (3.79%) and Mining Investments LLC (96.21%), which is chaired and co-chaired by Dimitri Troitsky and Dimitry Korzhev, respectively; both of whom hold Russian citizenship. Dimitri Troitsky also owns Eulachon Limited, the parent company of Mining Investments LLC. Troitsky ranks 184th among Russia's richest businessmen.
LTD Capital Group holds a gold mining license for the period of 2019-2044.	The owner of 50% of the company shares, Pridon Katamadze, is a dual citizen of Georgia and Russia, who is also associated with a project for constructing an artificial island in Batumi.
Mega Holding (Tbilcement Group) has a license for stone gravel extraction for the period of 2020-2025. Mega Holding includes concrete manufacturers and construction companies that produce 120 cubic meters of concrete and 14 tons of cement.	A 50% share in Mega Holding is held by Iveria Pro LTD (solely owned by Iveria Invest LTD). A Russian company Ost Intertrade LTD, a Lithuanian company LIS Group, and a Russian citizen, Nadezhda Obitotskaya, own a total of 49% of Iveria Invest LTD. Notably, the registered addresses of Ms. Obitotskaya and the two legal entities are identical.
Sairme Mineral Water holds three licenses: for freshwater (2010-2030), underground freshwater (2011-2036), and carboard mineral water (2019-2031).	Russian citizen, Yakov Gvichia, has 100% ownership, while a supervisory board member, Gia Gvichia, is a top Russian billionaire.

IDS Borjomi extracts and produces the mineral and still waters of Borjomi, Likani, Borjomi Springs, and Bakuriani.	Between 2013 and 2022, Russian sanctioned billionaire, Mikhail Fridman held the controlling share in the company. Nevertheless, since the start of the full-scale Russian war against Ukraine, there have been modifications to the ownership structure of IDS Borjomi. Specifically, due to the sanctions regime, Fridman's shares decreased by 7.73%, and corresponding shares were transferred to the Georgian government. Due to this transfer, Fridman lost controlling rights in IDS Borjomi.
Gruzvinprom holds a mineral waters extraction license. Another company, Melikishvili Inn, is affiliated with Gruzvinprom. These companies received the greatest amount of money from simplified public procurements in 2020.	Gruzvinprom is owned by Bolero & Company, the sole shareholder of which is a dual Russian and Georgian citizen – Vakhtang Karichashvili. He owns Melikishvili Inn with Ucha Mamatsashvili, a relative of Bidzina Ivanishvili, and a dual citizen of Georgia and Russia.
Mixor holds a mineral waters extraction license.	Temur Anchabadze, a businessman from St. Peterburg is a shareholder of the company and owner of Keystone Investments LTD. Anchabadze is also the founder of the Russian North European Gas Pipeline Logistics company. Keystone Investments is linked with the South Stream project, supplying natural gas to Europe and transporting gas within Russia.

The assessment of Russian business linkages within the Georgian mining and mineral waters sector thus indicates moderately concerning signs and sphere vulnerability from potential risks due to the current extent of Russian ownership. Since the ownership shift in IDS Borjomi, Russian interests in this sector have technically decreased. Nevertheless, as this sector has high employability potential, together with its significant economic and societal value, its vulnerabilities towards the potential threats associated with Russian ownership are heightened.

BANKING, TOURISM, CONSTRUCTION, AND TRANSPORTATION

Lastly, there has been no significant Russian ownership discerned in terms of the banking, tourism, construction, or transportation sectors. The banking sector includes Georgia's VTB bank, the total capital of which reached 4% of the Georgian market in 2020. The Russian VTB Bank owned 97.38% of VTB Georgia. Although, since the war in Ukraine, VTB has transferred its portfolios to other Georgian banks (Institute for Development of Freedom of Information (IDFI), 2023, p. 12).

In the tourism and hotel industry, as well as the construction and transportation sectors, the IDFI identifies no significant Russian ownership. According to the information available, out of 20 medium-sized construction companies on the Georgian market, only three have Russian linkages, while in the transportation sector 10% of medium-sized companies (36 companies) belong to Russian citizens (Institute for Development of Freedom of Information (IDFI), 2023, pp. 5-7).

Overall, considering the eight sectors studied by the IDFI, as of June 2023, concerning signs of Russian ownership are particularly visible in Georgia's electricity sector, followed by oil and natural gas, communications, and mining and mineral waters. However, there is low to non-existent concern regarding ownership structures in the banking, tourism, construction, and transportation sectors. Nevertheless, it is conspicuous that business ownership in these sectors has been modified in parallel with Russia's war in Ukraine and the corresponding sanction packages. As a result, direct Russian linkages in Georgian businesses have, legally, diminished since the spring of 2022. Nevertheless, disregarding these shifts, details of the deals regarding ownership changes have still not been disclosed, thus leaving doubts regarding the remaining Russian influence in the various companies and sectors reviewed.

Table 3: *Russian ownership assessment per sector (as of June 2023)*

SECTOR	OWNERSHIP ASSESSMENT
Electricity Generation, Supply, Transmission	Significant influence can be traced through Russian citizens or businesses that directly own or might control electricity generation (Khramhesi 1 & 2, Mtkvari HPP, Dariali HPP, Skurdidi HPP, possible involvement in management of Enguri HPP), supply (Telasi/Telmico), transmission (Sakrusenergo JSC), and trade (Lux Energy Trading LLC)
Oil and Natural Gas	Noticeable influence can be traced through one of the five top retail oil operators, Lukoil, with Russian ownership, and one significant player on the market, Petrokas, previously having strong Russian ties
Communications	Moderate influence is traceable through Fridon Injia's interest on the market, and Veon Georgia having had notable Russian ties
Mining and Mineral Waters	Moderate influence can be traced through several license-holders with clear Russian connections (RMG, IDS Borjomi, Sairme Mineral Waters, Gruzvinprom, Mixor, Capital Group, Tbilcement Group)
Banking, Tourism, Construction, Transportation	Low to non-existent ownership-related influence, with some sectors increasing the trend of dependency

Source: *IDFI; Authors' elaboration*

LITERATURE REVIEW

The following sections explore specific risks related to the current extent of Russian ownership within Georgian business. First, based on a literature review, we contextualize the topic by studying Russia's role as a threat actor in the global and the Georgian contexts. Thereafter, we provide an overview of the literature that refers to the hybrid threat of foreign ownership from malign state actors. We place particular emphasis on those threats of foreign ownership related to critical infrastructure and the capturing of critical infrastructural sectors.

RUSSIA – A GLOBAL THREAT ACTOR WITH HYBRID TACTICS

Among unconventional threats, hybrid tactics deserve special attention due to their encompassing nature. These threats involve a wide array of synchronized and deliberate actions, utilizing both familiar and novel tools in innovative ways, each driven by malicious intent (Giannopoulos, Smith, and Theocharidou, 2021). According to the European Centre of Excellence for Countering Hybrid Threats, such threats refer to those actions carried out by state or non-state actors aiming to undermine or harm a target by exerting influence over its decision-making processes at the local, regional, state, or institutional level (Normark, 2019).

Hybrid tactics have been an integral part of the Kremlin's arsenal for a long period. In a publication from 2013, Valery Gerasimov, the Chief of the General Staff of Russia, put forth the notion that "the very 'rules of war' have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness" (Gerasimov, 2013). While some experts have downplayed the significance of Gerasimov's article, it has been widely interpreted in the West as a clear articulation of Russia's hybrid strategy (Galeotti, 2018).

The Russian leadership has also referred to employing hybrid tactics in official documents, including, most recently, the 2021 National Security Strategy, which states that Moscow considers it legitimate to take the symmetric and asymmetric measures required to suppress unfriendly actions and to prevent their recurrence in the future. The Kremlin argues, however, that hybrid conflict is not one-sided since the West has also been adopting similar tactics against Russia. In January 2023, the Russian Foreign Minister, Sergey Lavrov, argued that the war in Ukraine represented a response to the hybrid war unleashed by the West, while Dmitry Peskov, Press Secretary of the Russian president, predicted that the "hybrid war of hostile countries against the Russian Federation" will continue for years (Rawan & White, 2022).

Russia has employed hybrid tactics in various instances across Europe, including in the Georgian context. The most complex and comprehensive examples of Russia's hybrid tactics have been tested in Ukraine. Prior to the full-scale war in Ukraine, these tactics were evident during the annexation of Crimea and the intervention in eastern Ukraine in 2014, where unmarked soldiers – 'little green men' – were utilized. Furthermore, Russia systematically targeted Ukrainian critical infrastructure

through both physical and cyberattacks over a prolonged period. During the war, Russia's deliberate attacks on Ukrainian energy infrastructure even amount to war crimes (Amnesty International, 2022).

Russia has equally employed hybrid attacks against other European nations. In 2014 and 2015, it was alleged that Russia was involved in detonating ammunition depots in the Czech Republic and in Bulgaria. Additionally, Russia has been accused of interference in various elections and has launched numerous disinformation campaigns across the region. These actions again highlight the utilization of hybrid strategies to exert influence and to disrupt the stability of European countries.

Annex 1 below provides a short list of suspicious incidents that were potentially backed by Russia across Europe in 2022. These episodes represent just a few cases among many suspicious events. Crucially, such occurrences provide substantial evidence suggesting that Russia acts as a global threat actor. These incidents also highlight Russia's capability and willingness to engage in actions that pose risks to the security and stability of critical infrastructure throughout Europe.

Overall, the events surrounding the Russian invasion of Ukraine and incidents of suspected sabotage have raised the level of concern regarding the protection of critical infrastructure, thus prompting calls for enhanced measures and heightened vigilance to counter potential threats.

RUSSIA'S HYBRID TACTICS – A THREAT TO GEORGIA'S SECURITY

Beyond its global actions, Russia represents an existential threat to Georgian security as it utilizes both conventional and unconventional instruments to disrupt and damage the stability of the country. Russia has occupied and continues to maintain control over Abkhazia and South Ossetia, which are internationally recognized as part of Georgian territory. Crucially, Russia's military presence in the occupied regions of Abkhazia and South Ossetia directly threatens Georgia's security. There have been instances of border violations, military build-ups, and occasional skirmishes, which each contribute to a state of instability and tension. Russia has moreover provided support to separatist movements within Georgia, thereby fueling conflicts and undermining the country's territorial integrity; this support includes military assistance, weapon supplies, and political backing for separatist leaders (Modebadze, 2019).

In addition to military aggression, Russia has been known to engage in extensive malign information operations targeting Georgia. Significantly, the utilization of hybrid tactics has intensified since Russia launched its war against Ukraine. These hybrid efforts aim to shape public opinion, manipulate narratives, and create divisions within Georgian society. Moreover, Russia maintains influence over local political and social dynamics by supporting pro-Russian political parties, pro-Russian media platforms, funding sympathetic organizations, and promoting Russian cultural and language ties. This influence can be used to shape policies, destabilize the government, and undermine Georgian sovereignty (Adzinbaia & Zawadzka, 2018).

Disinformation campaigns potentially linked to Russia and pro-Russian actors have taken various forms. For example, possibly one of the most damaging disinformation campaigns targeted the Tbilisi-based Richard Lugar Center for Public Health Research during the initial stages of the COVID-19 pandemic, in which the center was blamed for the preparation of biological warfare.

In September 2004, Moscow imposed a complete transportation blockade on Georgia, including the closure of Russian airspace. While these actions were ostensibly framed as debt collection measures against Georgian entities, they were perceived as punitive measures targeting Georgian associations with commercial interests in Europe and the United States.

Furthermore, in 2006, Russia disrupted natural gas and electricity supplies to Georgia, virtually banned Georgian exports to Russia, and initiated the deportation of Georgian citizens. These actions severely impacted the Georgian economy. Additionally, on 15 August 2008, a strategically important railway bridge in Kaspi was destroyed, and a fire erupted in the Borjomi National Park, an important tourist destination. These acts were considered as provocative and the blame was assigned to Russia (Dayspring, 2015). After the events of "Gavrilov's nights'" anti-government and anti-Russia protests in Tbilisi of 20 June 2019, Russia decided to "punish" Georgia and banned flights to the country. This form of economic coercion is thus used as a tool to influence Georgian politics and to deter the country from pursuing closer ties with the West (TI Georgia, 2022).

There have equally been several cases of high-profile cyberattacks attributed to Russian actors. These attacks, disrupting operations and compromising sensitive information, have targeted government institutions, critical infrastructure, and media outlets.

Most significantly, the Kremlin, as the center of political power in Russia, has been known to use its energy policy as a tool for achieving its strategic objectives multiple times. Annex 2 provides examples in which Russia has used its energy leverage for political purposes in Georgia.

Utilizing a combination of military, political, economic, informational, and proxy tools to exert influence, destabilize the country, and challenge its sovereignty, these factors collectively demonstrate that Russia represents an existential threat to Georgia's security. Considering this adversarial stance and the employment of threatening hybrid strategies, it is imperative to evaluate the risks associated with Russia's multi-dimensional presence in Georgia, including its role and interests in the Georgian economy.

The risks stemming from Russian business ownership within the Georgian economy have never been fully researched. Nevertheless, analyzing these risks provides a foundation for the development of an operational policy framework for effective risk mitigation strategies. By considering the broader context and understanding the intentions behind Russian actions, policymakers and stakeholders can make informed decisions to help safeguard Georgia's security interests, protect its critical infrastructure, and mitigate potential vulnerabilities stemming from Russian ownership in Georgian businesses.

FOREIGN OWNERSHIP – A HYBRID THREAT

Exploiting global stakes in business ownership to expand its area of influence can be regarded as one of the central means for the Kremlin to affect the normality across various national contexts. Besides business rationale, foreign ownership can be considered a form of hybrid threat due to its potential to combine dimensions from both the economy and security, thus creating risks that are not solely limited to traditional military threats.

Foreign ownership blurs the line between economic interests and national security objectives. Therefore, to safeguard national security interests, governments need to consider not only traditional military threats but also the broader spectrum of risks associated with foreign ownership (Arnold & Delgado, 2019).

Foreign entities may acquire ownership stakes in critical sectors or industries, ostensibly for economic purposes, while also having the potential to exploit their positions to advance strategic, political, or security interests, those which may not align with a host country's objectives. Foreign ownership can exploit a host country's economic dependency by leveraging ownership positions to exert economic pressure, to manipulate prices, or to disrupt essential services. Such economic manipulation can impact a nation's stability, compromise critical sectors, and undermine its security. In conflict situations or geopolitical disputes, hostile actors can also employ foreign ownership as a hybrid tactic. It can be used to gain influence, control strategic assets, destabilize economies, or instigate further territorial ambitions, thus blurring the lines between military and non-military action (Larson & Marchick, 2006).

One concern regarding foreign acquisitions may arise when there is evidence that a company is under the control or influence of a foreign government with hostile intentions towards its host country. In other cases, concerns may stem from the necessity for such companies to collaborate with the host country's security or intelligence agencies and to handle sensitive information responsibly. Certain situations may arise where the nationality of the acquiring firm raises security issues that necessitate examination and, if required, appropriate action.

Table 4: *Potential risks associated with foreign ownership*

Economic Dependencyand Manipulation	Extensive foreign business ownership can lead to a host's economic dependency on other nations. Foreign owners can influence or manipulate domestic markets, trade policies, and financial systems for their own gain. This may undermine a country's economic stability, impact national security, and compromise industries vital to defense or national interests.
Technology Transfer	Foreign ownership can facilitate the transfer of sensitive technologies, intellectual property, and know-how to other countries. If these technologies have military applications or can be used against national interests, they may compromise a nation's defense capabilities and its strategic advantage.
Espionage and Cybersecurity Threat	Foreign ownership can provide opportunities for espionage and cyberattacks. Entities with access to critical infrastructure or sensitive information can exploit their ownership positions to gather intelligence or to launch disruptive cyber operations, thus undermining national security.
Supply Chain Vulnerabilities	Reliance on foreign-owned companies for essential goods, services, or raw materials can create vulnerabilities in the supply chain. Disruptions caused by foreign owners can affect sectors crucial to national security, such as defense, healthcare, or communications.
Political Influence	Foreign ownership can potentially grant foreign entities undue political influence within a country. They may seek to shape national policies, impact decision-making processes, or manipulate public opinion to advance their own interests, and which may not align with a host nation's security objectives.
Dual-use Technologies	Foreign-owned companies engaged in the research, development, or production of dual-use technologies (civilian and military) can raise concerns. The misuse or diversion of such technologies by foreign owners can compromise national security or enable potential adversaries to develop advanced weaponry.
Strategic Assets Control	Foreign ownership of strategic assets such as ports, airports, or critical infrastructure can impact a nation's ability to control and safeguard its borders. In certain cases, this could potentially be exploited to facilitate illicit activities, like smuggling or unauthorized access to sensitive areas.

It is important to note that not all foreign ownership poses significant national security risks, and the specific risks depend on factors such as the nature of the industry, the country involved, and the intentions of the particular owner. For example, it is difficult to perceive how foreign ownership of businesses involved in real estate, retail, or agriculture, for instance, could pose a threat to national security interests. Therefore, the challenge lies in identifying the acquisitions that genuinely raise security concerns and, whenever possible, finding ways to address and mitigate those concerns (Larson & Marchick, 2006).

In order to accurately identify the threats related to foreign ownership, it becomes significant to analyze the presence of foreign ownership through the prism of critical infrastructural protection. Foreign direct investments represent the cornerstone of the Georgian economy. Thus, it is of utmost importance to accurately contextualize the risks related to foreign capital accumulation in the country. Nevertheless, we argue that foreign ownership within critical infrastructure (CI) must be treated as especially concerning for the various reasons indicated below.

To represent ownership-related risks within critical infrastructure, we first offer an overview of the definitions, sectors, and criteria for identifying CI. As there is no holistic legal definition of CI in Georgia, we base our analysis on international experiences matched with the local context.

CRITICAL INFRASTRUCTURE – DEFINITIONS, SECTORS, AND CRITERIA

There is no universally accepted definition of "critical infrastructure" – the term itself is relatively new and its scope is still in the process of evolution. Generally, the notion refers to those areas of public life that are important for national security and are so significant that, if endangered, the normal course of life and the safety of citizens will be in question (Mitrevska, Mileski, & Mikac, 2018, p. 19).

It is hardly surprising that the existing definitions of CI vary across different jurisdictions (Annex 3 provides definitions of critical infrastructure within the European Union, the United States, Australia, Germany, the United Kingdom, and Canada). While in many countries, a legal definition of CI is still non-existent. According to the available definitions, the "criticality" of infrastructure is determined by the scale of negative impact that would be generated nationwide (or across nations) in cases of failure, incapacity, degradation, or destruction.

Alongside such definitions, we can moreover identify sectors that are generally perceived as having critical significance to national security as well as to societal and economic integrity. Although the list of critical sectors differs for each country, even in the very narrow list (for example, under the definition used in the European Union), the energy and transport sectors are regarded as highly critical[4]. These are followed by communications, food, finance, water, health, IT, emergency services, and other sectors like chemicals, dams, defense, government facilities, etc.

[4] In terms of the definition accepted in the European Union, EU-wide critical infrastructure might also cover other sectors, those in which critical facilities might have negative consequences on at least two member states simultaneously. However, the energy and transport sectors are mandatorily assessed as having high security significance.

Table 5: *Critical infrastructural sectors in the European Union, the United States, Australia, Germany, the United Kingdom, and Canada*[5]

	European Union	United States	Australia	Germany	United Kingdom	Canada
ENERGY	O	O	O	O	O	O
TRANSPORT	O	O	O	O	O	O
COMMUNICATION		O	O	O	O	O
EMERGENCY SERVICES		O			O	
INFORMATION TECHNOLOGY		O		O		O
FOOD		O	O	O	O	O
FINANCE		O	O	O	O	O
WATER		O	O	O	O	O
HEALTH		O	O	O	O	O
OTHER		O	O	O	O	O

Source: *Authors' elaboration*

Significantly, as the security landscape is changing, more and more sectors and industries are covered by the concept of "critical infrastructure". Even within the European Union, where a conservative definition of union-wide critical infrastructural sectors has been adopted, the EU Commission recommends broadening the list of sectors to cover industries including banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public

[5] Grey color in the table denotes sectors that are assumed to be mandatorily critical

administration and space (European Parliament, 2021, p. 12) to respond properly to the arising security challenges.

Threats that affect the secure and resilient operation of critical infrastructure are often complex and unpredictable. Moreover, threats transform and evolve with the time. Although traditionally threats were associated with physical vulnerabilities and natural hazards, at present one major threat relates to cyber risks. The increased vulnerability of critical infrastructure against cyber risks is precipitated by notable progress in the management and coordination of information and communication technologies. In addition, increasing interdependence among sectors inside a country, or countries of a region, further increases this threat and the respective vulnerability.

Intentional disruption to the operation of critical infrastructure or that caused by natural hazards can instigate a chain reaction and paralyze the supply of essential services. This can trigger major threats to the social, economic, and ecological security and the defense capacity of a state. The following are certain key factors that underscore the fragility of critical infrastructure:

Essential Services: Critical infrastructure refers to physical and virtual systems and the assets that are vital for the functioning of society and the economy. This includes sectors such as energy, water, transportation, telecommunications, healthcare, and finance. Disruptions or damage to these sectors can have severe consequences on public safety, economic stability, and social order.

Wide Accessibility: Critical infrastructure is designed to be accessible and to provide essential services to a large population. This accessibility, while crucial for the smooth operation of society, also makes it vulnerable to attacks. The widespread presence and the interconnection of critical infrastructure make it easier for potential attackers to identify and target specific assets.

Interdependence: Critical infrastructural sectors often rely on each other, forming an interconnected web of dependencies. Disrupting or damaging one sector can have a cascading effect on others, thus amplifying the impact, and potentially causing a domino effect. This interdependence increases the vulnerability of critical infrastructure as a whole and magnifies the potential consequences of an attack.

Physical Vulnerability: Critical infrastructural assets often have physical vulnerabilities that can be exploited. For example, power plants, water treatment facilities, or transportation hubs may have limited security measures, making them susceptible to physical attacks, sabotage, or unauthorized access. Infrastructural elements like bridges, tunnels, or pipelines can also be targeted due to their accessibility and strategic importance.

Vulnerability to Natural Disasters: Critical infrastructure is often particularly vulnerable to natural disasters, which may cause destruction or total incapacitation of the infrastructure. The interdependent nature of CI further heightens the severity of this threat. As such, countries utilize disaster risk management strategies to adequately deal with such vulnerabilities.

Reliance on Information Technology: Modern critical infrastructure relies heavily on information technology (IT) and operational technology (OT) systems for efficient operation and management. This dependence on IT and OT introduces additional vulnerabilities, as these systems can be targeted through cyberattacks. Successful cyberattacks can disrupt operations, compromise safety mechanisms, and facilitate unauthorized access to critical infrastructure assets.

Economic Impact: Disruptions to critical infrastructure can have significant economic consequences. Industries, businesses, and supply chains depend on the reliable functioning of this infrastructure to operate effectively. Any disruption or damage can result in financial losses, reduced productivity, and economic instability, making critical infrastructure an attractive target for those seeking to inflict harm or exert influence.

Symbolic Value: Critical infrastructure often holds symbolic value due to its importance and visibility. Attacking or damaging iconic infrastructural assets can generate media attention, create fear and panic among the population, and convey a message of vulnerability or weakness.

Given these factors, critical infrastructure requires robust security measures, preparedness, and resilience strategies to protect against potential threats and to mitigate the impact of attacks. Consequently, governments and the organizations responsible for critical infrastructure should invest in risk assessment, threat detection, physical security measures, cybersecurity protocols, and contingency plans to safeguard these vital assets (OECD, 2008).

Certain threats cannot be predicted in advance. Nonetheless, the ability to identify existing threats and anticipate potential trends is vital for ensuring the security of critical infrastructures. For instance, cyberattacks targeting energy providers have the potential to cause various detrimental effects, including power outages, power surges, destruction of equipment, and damage to devices across the grid. Additionally, natural disasters, such as floods or severe storms, can significantly impact national energy and transportation sectors, resulting in service disruptions due to extensive damage (European Parliament, 2021).

The protection of critical national infrastructure entails the establishment of a comprehensive framework that encompasses the identification, definition, and listing of infrastructure considered critical at the national level. This framework can equally serve as a basis for understanding the vital sectors and assets that are central for a nation's functioning, security, and resilience.

GEORGIA-SPECIFIC RISKS OF RUSSIAN BUSINESS OWNERSHIP

Before analyzing the specific risks that stem from the current extent of Russian ownership in Georgian businesses, it is important again to consider the sectoral snapshot of Russian capital accumulation within Georgian commercial entities in order to understand the criticality of sectors and infrastructure in which Russian ownership stakes are concentrated.

Significantly, as this research is based on the previous IDFI findings, it specifically looks at the presence of Russian ownership in Georgian businesses across eight sectors of the Georgian economy, namely, electricity (generation, supply, transmission, and trade); oil and natural gas; communications; mining and mineral waters; banking; tourism; construction; and transportation. At present, significant Russian influence can be seen in the electricity sector, noticeable influence is present in the oil and gas sector, while a moderate influence is found in the sectors of communications and in mining and mineral waters. Whereas in the remaining sectors – banking, tourism, construction, and transportation – little to no influence was detected in the latest IDFI research.

Evidently, Russian ownership in Georgia is concentrated in sectors with strategic importance for Georgia's national security and its economic resilience. In other words, we can trace Russian ownership in critical infrastructural sectors, particularly in energy and communications. Even though Georgia does not have a legal definition of its own CI, it can be noted that the we can observe Energy and Communication sectors are regarded as critical in numerous national contexts. In terms of the energy sector, its significance can also be acknowledged in the supranational context of the European Union. Moreover, while Petrocas's formal linkages are no longer present at Poti oil terminal, their footprint alongside San Petroleum Georgia and Gulf Aviation, together with Lukoil Georgia as a leading player on the oil retail market, underscores the vulnerability in the oil and natural gas sector. Lastly, ownership in the mining sector also deserves attention considering its high societal and environmental significance, and its notable potential employability in its various corresponding activities throughout Georgia.

In summary, Russian ownership within the Georgian economy is particularly threatening due to ownership within sectors that have critical significance for the overall security and the economic resilience of the country. Identifying and assessing the Georgia-specific risks associated with Russian business ownership provides a useful foundation for potential policy responses.

Based on the relevant literature and a series of expert interviews, we identify below, due to their corresponding vulnerabilities and impacts, the threats that will be later in this report evaluated considering their severity levels. Significantly, these threats are not solely limited to potential physical damage of infrastructural assets from the deliberate destabilization of networks, military attacks, terrorism, or sabotage, they also include other types of vulnerabilities derived from political influence, economic manipulation, espionage, among other factors. Historic Russian hostility dictates that Russia can impose physical damage and tangible harm on critical infrastructure,

disregarding its own stake in such assets or commercial entities. Thus, although we argue that physical vulnerabilities, like sabotage, might be amplified in cases of Russian ownership, it appears predominantly to be intangible, hybrid influences that deserve special attention and further regulatory treatment.

POLITICAL INFLUENCE

Russia does not adhere to a market economy model; rather, its business operations are closely intertwined with the objectives of the political establishment. This interconnection makes it challenging, if not impossible, to differentiate between the motivations of Russian business and the political elite. Consequently, there is a substantial likelihood that Russian ownership in Georgian businesses, especially within sectors of critical significance, could serve as a channel for exerting political influence.

Gerasimov's doctrine explicitly stipulates that non-military tactics, which encompass economic means of influence, have become Russia's "preferred way to win," thus effectively constituting actual conflict itself (McKew, 2017). Therefore, it is logical to be sceptical regarding an absence of political motivations behind Russia's business presence in Georgia.

These motivations are particularly visible when examining business connections that are directly linked to Russian billionaires who hold ownership stakes in Georgian enterprises. Such strongmen not only maintain direct political affiliations with the Russian elite but are also tied to money laundering schemes and Russian military undertakings within its "areas of influence". As an illustration, Mikheil Fridman, a significant player in Georgia's communications and it mining sector, was detained in the United Kingdom on suspicion of money laundering (Politico, 2022). Furthermore, Fridman has recently been associated with the insurance of Russian military vehicles employed during the conflict in Ukraine. Notably, a separate entity under his management also operates a joint venture that supplies the Russian Defense Ministry with essential services like food and clothing (RFERL, 2023). Mikhail Fridman has been sanctioned for directly supporting the invasion of Ukraine financially.

The threat of Russian infiltration into Georgian politics via business ownership is particularly notable in the case of Fridon Injia, whose family controls 24.19% of the Georgian landline telephone market and 6.2% of the fixed internet connection market. Injia, an MP in the current convocation of the Georgian Parliament, has consistently been one of the most anti-Western and most pro-Russian MPs. represents an outspoken supporter of the anti-Western agenda during the current term of Georgian parliament. He previously also used to finance the political party "Alliance of Patriots", which directly advocated for recovering diplomatic relations between Georgia and Russia, condemning Georgia's Euro-Atlantic aspirations and calling for Georgia's military neutrality.

Evidently, the intertwining of business and political interests has the potential to disrupt internal dynamics, to undermine democratic processes, and to foster toxic political sentiments within

Georgian society. Moreover, this substantial degree of political influence has the capacity to undermine Georgia's aspirations to join NATO and the European Union.

EXPORTING CORRUPTION

Another threat connected to notable Russian businesses ownership lies in the potential to nurture corrupt practices. Such a threat is amplified due to the regulatory context in Georgia, which lacks institutional checks to curb corruption and to effectively deter the vested interests of different parties. There have been several threats of this nature, including 'revolving door' incidents[6], tax evasion, and exploitation of the public procurement system; with documented cases of such in both the Georgian and the broader context.

According to Transparency International (TI), of the several recorded revolving door incidents, one relates to Inter RAO Georgia LLC, a joint Russian and Georgian business. One day after it commenced operations in May 2019, Inter RAO Georgia LLC was registered as a participant of the wholesale trade and supply of electricity by the state-owned enterprise Electricity Market Operator JSC (ESCO)[7]. Through Inter RAO Georgia LLC, ESCO moreover became involved in importing Russian electricity. Critically, Vakhtang Ambokadze, who was appointed as a director of Inter RAO Georgia LLC, served as Director General of ESCO until the first day that Inter RAO Georgia LLC received registration (Transparency International Georgia, 2023).

Besides such revolving door cases, Russian-owned companies have a track record of tax evasion. In 2018, Armenian law enforcement agencies raided the offices of South Caucasus Railway (SCR) over allegations of tax evasion and the inflation of the volume of its capital investments by 400 million drams. Later in 2018, another fraud inquiry was launched against the Armenian gas distribution network, owned by Russian Gazprom. The distribution network was accused of evading millions of dollars in tax (RFERL, 2020). Although these disputes were each 'settled', they plainly manifest the corruption risks to commercial entities under Russian management, including those of critical significance.

In Georgia, Russian ownership has been further associated with exploitation of the national public procurement system. According to IDFI findings, Lukoil, the Russian-owned retail oil operator, has actively been participating in public tenders; between 2010-2022 they signed procurement deals worth some 200 mln. GEL. Moreover, Lukoil Georgia and Otar Partskhaladze, who served as a deputy director, were alleged to be participating in an corrupt scheme that blocked the transportation of oil products through Georgia to Armenia.

[6] The term "revolving door" refers to the movement of upper-level public officials into high-level private-sector jobs, or vice versa. Significantly, such movement occurs in private industries that are regulated by the respective public sector agencies, where public officials were employed.

[7] ESCO exclusively pursues the Balancing Electricity and Guaranteed Capacity trading and fulfills the seasonal need for import/export of electricity and inspects the wholesale metering nodes in Georgia.

Nurturing corrupt practices not only spoils the internal business environments, but it also discourages the inflow of future investment; this is particularly true of efficiency-seeking investments that contribute to capital inflow and job creation, which also foster innovation and technology transfers and boost export capacity, market diversification, and human capital development.

ECONOMIC DEPENDENCY AND MANIPULATION

A heavy concentration of foreign ownership in any sphere, especially in spheres of critical significance (like energy, telecommunications, or transport) creates the risk of "sphere capture," when foreign actors receive leverage to disrupt the normality within a "captured sector" by manipulating with economic instruments, such as prices. Any heavy foreign ownership presence might additionally create supply chain vulnerabilities, those which have the potential to disrupt the provision of the essential services that are crucially important for society.

The significant presence of Russian ownership in Armenian critical infrastructure sectors shows how this threat manifests itself. Russia has exceptional leverage over the Armenian energy sector, including through high ownership stakes. Armenia meets more than 80% of its natural gas demand through Russian imports – this amounted to 2.6 billion cubic meters in 2022, 6.1% higher than the respective imports in 2021 (ARKA News Agency, 2023). Equally, since February 2014, Russian Gazprom has formally become the full owner of the Armenian natural gas distribution company, Gazprom Armenia.

Although Armenian dependency on Russian gas has always been high, arguably the presence of Russian ownership in the Armenian gas distribution network has created additional leverage for manipulation of the sphere via gas prices; despite constant negotiations between Russian and Armenian counterparts, gas prices have spiked several times in Armenia. Ironically, Russia openly utilized a price manipulation strategy after Armenia communicated its EU aspirations, and prices then reduced after Armenia's accession into the Eurasian Economic Union (EEU) (Terzyan, 2018).

In the case of the South Caucasus Railway, the sole railway operator in Armenia, Russia threatened Armenia that it would terminate its operations following fraud allegations against the company in 2018 (RTVI, 2019). As a resolution to this dispute, parties negotiated to ensure that South Caucasus Railway continued operations in Armenia.

In Georgia, Russian business ownership comparable to Armenia can be seen within the electricity sector. The energy sector, including the electricity, natural gas, and water industries, is regulated by the Georgian National Energy and Water Supply Regulatory Commission (GNERC). GNERC monitors market dynamics, including via setting and regulating tariffs for electricity, natural gas, and water. Thus, we might assume that manipulation with tariffs will be partly deterred in Georgia given the presence of GNERC. However, as observed in the Armenian case, the presence of the national regulator, the Public Services Regulatory Commission (PSRC) of the Republic of Armenia, still does not have a significant impact on Russia's price manipulation strategy.

In the case of the Georgian electricity industry, the risk of economic manipulation is further heightened because of the simultaneous presence of Russian footprint in several aspects of the sector – such as generation (e.g., Khramhesi 1, 2), supply (e.g., Telasi JSC), transmission (e.g., Sakrusenergo JSC), and electricity trading (e.g., Lux Energy Trading LLC, formerly known as Inter RAO Georgia LLC). Such simultaneous Russian footprint in different parts of the interdependent electricity system might therefore create additional risks of economic manipulation.

ESPIONAGE

Another potential threat related to Russian business ownership in Georgia is connected to various forms of espionage, including economic and cyber espionage. In other words, Russian ownership might be a channel for transferring sensitive information from Georgia to Russian intelligence agencies. Such information might include company-related data (e.g., commercial information), like trade secrets, intellectual property, and other confidential details. Furthermore, espionage may target consumers of the company and leak their personal information, which may later be used for different means, including within disinformation campaigns that can influence public opinion, impact election results, and even spoil Georgia's democratic standing. Additionally, espionage regarding critical networks, including different energy and infrastructural networks, has potential to facilitate potential acts of sabotage.

The risk of espionage is heightened since Russian ownership is present in critical infrastructural sectors of the Georgian economy, such as energy. Espionage related to critical infrastructure is of particular alarm considering the various vulnerabilities within CI, including physical vulnerabilities, its high societal significance, as well as their various interdependencies. For instance, espionage related to the confidential information of Telasi JSC could have the potential to affect over 600,000 subscribers in the Georgian capital.

This threat is further elevated as representatives of Russian-owned businesses have close political and business affiliations. In certain cases, these representatives are simultaneously present as decision-makers in strategically significant positions. For example, IDFI research reveals that a high-level official in a Russian-owned commercial entity (Mtkvari Holding LLC) in Georgia also acts as a supervisory board member within a single electricity transmission system operator in the country. Thus, "revolving door" incidents have also become significant in this regard.

Spying and espionage have long been among Russian methods of infiltration in different political and economic environments globally. From the numerous suspicious and proven cases of spying, there are recorded instances that definitively relate to economic and industrial espionage. As such, there are concerns that Russian economic espionage highly correlates with the operation of Russian-owned business entities in several nations.

For example, according to a December 2022 report from the Swedish Defense Research Agency, properties under Russian ownership might have direct connections with illicit intelligence activities (FOI, 2022). In November 2022, underscoring a manifestation of these connections, the

Swedish Security Service (SAPO) detained a Swedish couple who had migrated from Russia, and they were accused of transferring secret economic information to Russian intelligence agencies. Significantly, the couple were business owners, specializing in trading of electronic components and industrial technologies (Le Monde, 2022).

Finally, as the latest example, it was discovered that Yandex GO, a Russian taxi operator that is active in Georgia, would begin to transfer the personal information of its customers to Russian intelligence agencies after September 2023: "The secret police will have unrestricted 24/7 access not only to information generated by their devices […], but also their user-generated data, including names, phone numbers, email addresses, bank accounts, user comments, and, of course, the addresses of their trips" (BMG, 2023). Consequently, this provides the potential to manipulate public opinion, to further exert influence over the information space, and to impact on democratic institutions and processes in Georgia.

SABOTAGE

Furthermore, sabotage and deliberate action to cause permanent or temporary incapacitation of targeted assets or networks is yet another risk when foreign ownership is present. In terms of sabotage, it would be naïve to believe Russian business ownership creates threats that would be totally absent without the ownership factor. On the contrary, in situations of heightened security, disregarding ownership, Russia certainly has the capacity to intentionally harm different sectors of the Georgian economy, including sectors of critical significance. Nevertheless, it would be safe to assume that such ownership simplifies acts of sabotage, especially for assets and networks of critical significance.

There have been numerous cases in which Russia has infiltrated various sovereign contexts via sabotage. For Georgia, the most prominent case of sabotage was recorded in the winter 2006, when Russia deliberately cut off the energy supply by incapacitating a gas pipeline and an electricity power line. This was followed by the banning of the main Georgian exports to Russia, the suspension of transport connections with Georgia, and the deportation of Georgian citizens from Russia.

Sabotage has remained a key instrument for Russia to damage other countries until this day. Before launching its full-scale war in Ukraine, the state targeted strategic Ukrainian facilities multiple times. For instance, the control centers of three Ukrainian electricity distribution companies were accessed remotely via cyber-sabotage in December 2015. As a result, more than 200,000 electricity subscribers lost power. In 2016, another substation was damaged in northern Kiev (Park & Walstrom, 2017). These acts of cyber-sabotage have often been associated with Russian government-affiliated hackers.

During the war, attacks that cause the deliberate incapacitation of critical infrastructure has emerged as a favored Russian tactic during its war on Ukraine. According to Amnesty International, attacks on critical Ukrainian infrastructure that led to nationwide blackouts amount to Russian war

crimes (Amnesty International, 2022). The recent destruction of the Kakhovka Dam is also thought to be a Russian act of sabotage, even though there is no definite proof.

In connection with the destruction of the Kakhovka Dam, two factors deserve attention. The first relates to the cascade effect triggered by this catastrophic event, as ultimately it led to the flooding of neighboring regions and inflicting significant environmental harm. This, in turn, could potentially result in increased grain prices and food shortages. Additionally, the disaster introduced the further risk of damage to the Zaporizhzhia nuclear plant. The second factor of note is the manner in which the dam was destroyed – from within rather than externally (The New York Times, 2023). This symbolically stresses the critical importance of bolstering the internal security of critical infrastructure. This task could potentially become yet more challenging when ownership and control of such strategic assets lies in the hands of adversaries.

In sum, in the context of Georgia, we argue that the presence of Russian ownership might simplify acts of sabotage, including cyber-sabotage, especially during times of heightened tension. There are various potential scenarios regarding the consequences of sabotage, including deliberate power outages through the incapacitation of power transmission lines and power supply infrastructure, and the damaging or destruction of electricity generation sites, affecting individual subscribers, businesses, and locations strategically significant for Georgia's security.

SANCTIONS AND SANCTION EVASION

The West's sanctions regime, which is targeted at Russian commercial entities and Russian elite groups, creates further, potentially impactful, risks associated with Russian business ownership in Georgian economic sectors. First, Russian-owned companies, through their owners, might themselves become targets of a sanction regime. Conversely, these businesses might also turn into havens for sanction evasion. Lastly, ownership shifts in response to sanctions might add to a lack of transparency regarding the management of these entities.

It is important to mention that following the introduction of the sanctions' regime, the official position of the Georgian government has been not to join Western sanctions and not to impose additional sanctions on Russia either. Up until now, the only area where Georgia automatically adhered to the imposed regime is banking and finance. As the country is part of the Western banking system, it does not need to introduce its own measures in this regard (Governance Monitoring Center , 2023, p. 16).

In light of sanctions regime, there have recently been two prominent cases of disturbed or suspended business operations in Georgia. In particular, relating to IDS Borjomi and VTB Bank Georgia. Such incidents enhance the country's vulnerability in several facets, though primarily they create economic susceptibility. As direct sanctioning targets, the commercial operations and financial resilience of both IDS Borjomi and VTB Bank Georgia shrunk significantly. The latter immediately suspended its market operations, while IDS Borjomi transferred a 7.33 percent share from the sanctioned Mikhail Fridman to the state – making Fridman formally lose his controlling

function. Although worse economic scenarios were effectively neutralized, in the long-term, the stable operation of Russian-owned business entities in Georgia remains questionable.

Notably, Russian-owned businesses significantly add to Georgia's economic growth. For instance, during each consecutive year from 2018 to 2022, mineral waters (including Sairme and Borjomi) reached the top five products domestically exported from Georgia. Moreover, Russian-owned businesses have the potential for high employability, especially within local contexts (e.g., mining sites outside Tbilisi), and thus have significance from a social security perspective. In terms of IDS Borjomi, the introduction of the sanctions regime created an immediate disturbance, manifested in enhanced uncertainty in terms of labor contracts, halved salaries, and lost jobs, each due to workers' unsuccessful negotiations with the company management (IWPR, 2022). Hypothetically, instability in Russian-owned businesses has the potential to cause social and political turbulence. Considering the probability of such turbulence, the Georgian state became the beneficial owner of 7.33% of IDS Borjomi, thus creating additional concerns regarding state intervention within private sector dynamics.

Another acute threat comes via the evasion of sanctions. It is likely that Russian-owned companies will be more prone to act as havens for Russia to evade sanctions, and to still offer access to revenues, sensitive goods, and technologies (e.g., dual-use technologies). Significantly, Georgia has officially aligned with various international sanctions. The latest report from the EU Sanctions Envoy, David O'Sullivan, was also positive regarding the inspection and monitoring systems in place for preventing sanctions evasion.

Lastly, amid the Western sanction regimes, there has been a trend for Russian-owned companies to change their beneficial ownership structure to avoid potential adverse economic and reputational impacts. In Georgia, this was observed in the case of Petrokas Energy and Veon Georgia. While such precedents are significant for future economic security in the Georgian business sector, they also add to the lack of transparency in management practices, a common trend in Russian-owned companies. Critically, according to our analysis, no details of the deals signed regarding recent ownership shifts in Georgia have, thus far, been disclosed to the public.

ASSESSING RISKS

In order to operationalize the research findings, we commissioned selected experts to rank each identified risk by two related yet distinct contexts. First, they assessed the level for each identified risk on a scale of 0 to 10; while taking into consideration Georgia's general economic dependency on Russia and Russia's local economic interests. In the second context, they assessed, on a scale from 0 to 10, the level to which Russian ownership increases the severity of each identified risk. These assessments were then grouped using simple averages (the findings from the exercise conducted are provided in Table 6 below).

Table 6: *Ranking exercise for identified risks*

IDENTIFIED RISK	OVERALL RISK LEVEL	LEVEL TO WHICH RUSSIAN OWNERSHIP ENHANCES RISK SEVERITY
RISK OF POLITICAL INFLUENCE	9.8	9.3
RISK OF SANCTIONS AND SANCTION EVASION	9.2	9.2
RISK OF EXPORTING CORRUPTION	9.5	8.8
RISK OF SENSITIVE INFORMATION OUTFLOW	8.8	8.8
RISK OF ECONOMIC DEPENDENCY AND MANIPULATION	8.5	9.2
RISK OF SABOTAGE, INCLUDING CYBER-SABOTAGE	8.5	8.5

Source: *Expert opinions; Authors' calculations*

The ranking exercise conducted suggests that the risk of political influence stemming from Russian ownership in Georgian businesses deserves the greatest attention, followed by the risks of exporting corruption, of sanctions and sanctions evasion, of sensitive information outflow, the risk of economic dependency and manipulation, and the risk of sabotage, including cyberattacks.

Significantly, the severity level for each identified risk is high. Nevertheless, if Russian business ownership is incorporated, the severity levels related to risks of political influence, of sanctioning and evasion, and for economic dependency and manipulation increase noticeably compared to the other factors. Compared to the overall risk level (excluding the ownership factor), the risk of economic dependency and manipulation is particularly elevated when the Russian ownership factor is represented. It is also notable that the risk of sabotage, including cyber sabotage, is assessed with the lowest score in each context provided. Disregarding Georgia's economic dependency on Russia or the presence of Russian ownership in the reviewed economic sectors, the latter judgment is logical considering Russia's military capacity and often malign motivations.

OVERVIEW OF RISK MITIGATION MEASURES

After identifying and assessing the Georgia-specific risks related to Russian private business ownership, it is necessary to discuss the potential measures to mitigate such risks.

Within the realms of critical infrastructure protection and foreign ownership, national strategies commonly employ a risk management framework. This approach enables governments to identify vital security assets, evaluate potential risks, and establish strategies and priorities for mitigating these risks. Typically, risk management strategies encompass actions to be taken within the key areas of prevention, preparedness, response, and recovery. These plans aim to enhance coordination among the appropriate government agencies and private sector operators responsible for critical infrastructural facilities, thereby effectively managing the associated infrastructural risks. Governments typically adopt an "all hazards approach," which entails scrutinizing threats to critical infrastructure originating from various sources, including natural disasters, accidents, and deliberate attacks.

Protecting critical infrastructure involves the active involvement of diverse actors. These actors encompass various international organizations and government agencies at different levels of governance. Additionally, the private operators of critical infrastructural facilities play a crucial role in all phases of this protection. Consequently, addressing the challenges related to critical infrastructural protection necessitates a wide range of expertise, and collaboration among these notable stakeholders (OECD, 2008).

The evaluation of risks to ownership in critical infrastructure is often case-specific, and it can be problematic to establish simple rules for such evaluation. Annex 4 provides a detailed overview of the tools used by various nations for risk assessment. General policy frameworks for critical infrastructural protection tend to take a comprehensive approach to risk – that is, programs cover major threats to infrastructure, regardless of the source of natural disasters, attacks, or sabotage, etc. However, not all countries have the national security or foreign intelligence capabilities required to make case-by-case evaluations of foreign investments in infrastructure.

It is important to note that the specific processes and mechanisms for assessing risk varies around the world, and each nation tailors its approach based on its unique circumstances, legal frameworks, and national security priorities. The test for establishing a potential threat in the context of foreign ownership typically involves assessing numerous factors to determine the likelihood and severity of risks to national security. While the specific tests and methodologies may differ among countries, some common elements are frequently considered, namely:

- ⇒ **Intentions and Motivations:** The assessment examines the intentions and motivations of the foreign owner. It aims to understand whether there is any indication of malicious intent, such as seeking control for strategic or adversarial purposes, or potential involvement in activities contrary to national security interests.
- ⇒ **Capability and Influence:** The assessment evaluates the capability and influence of the foreign owner to impact or disrupt critical sectors or national security assets. This includes analyzing their access to sensitive technologies, control over key infrastructure, ability to manipulate markets, or potential for espionage or cyberattacks.

- ⇒ **Adversarial Relationships:** The evaluation considers the foreign owner's relationship with other countries, particularly those that may be adversarial or have conflicting interests with the host country.
- ⇒ **Track Record and Behavior:** The assessment examines the past behavior and track record of each foreign owner. It considers whether they have demonstrated adherence to laws, regulations, and security protocols in their previous investments or acquisitions.
- ⇒ **Geopolitical Context:** The evaluation considers strategic considerations and the geopolitical context. It considers how foreign ownership may impact the balance of power, alliances, or regional stability.
- ⇒ **Impact on National Defense Capabilities:** The assessment considers the potential impact of foreign ownership on a country's defense capabilities and strategic advantage. It examines whether the acquisition of critical technologies, intellectual property, or defense-related industries may compromise military readiness, national defense, or sovereignty.
- ⇒ **Risk Mitigation Measures:** The evaluation includes an appraisal of the effectiveness of the proposed risk mitigation measures. If potential risks are identified, governments may impose conditions, restrictions, or mitigation measures to address those risks. The assessment also considers whether these measures are sufficient and practical in reducing the identified risks to an acceptable level.

It should be noted that these tests are part of a broader risk assessment process, and the specific elements and weighting of factors may vary among countries. Governments often conduct a case-by-case analysis to determine potential threats posed by foreign ownership based on the unique circumstances of each investment or acquisition; additional factors may moreover be employed subject to specific national security priorities and circumstances.

OVERVIEW OF INVESTMENT SCREENING MECHANISMS

Considering the available mechanisms that aim to ensure the resilient operation of national economic sectors, especially those of critical significance, one commonly employed tool is the screening of inward Foreign Direct Investments (FDIs) against their potential security implications. More and more economies globally are consequently conducting reviews of incoming financial transactions. As the Organization for Economic Co-operation and Development (OECD) notes, national investment screening policies have been adopted since the 1960s, however, such policies have become more popular in recent years (OECD, 2020). Nevertheless, typically the tool is targeted at pre-defined economic sectors of critical significance.

At least one-third of countries globally have some form of investment review procedure (Dechert LLP, 2022, p. 2). Data also shows that these are mainly developed economies, and often within the OECD, in which, as of 2022, 90% of members review their FDIs (Dechert LLP, 2022, p. 2). Within the European Union, 18 of 27 countries have adopted FDI screening measures; some countries are in the process of policy adoption under the latest EU Commission recommendation, which strongly advises EU members to review upcoming investment transactions (Dechert LLP, 2022, pp. 14-15).

The EU Commission was delivered alongside a recent EU-wide regulation – 2019/452 of the European Parliament and of the Council on Establishing a Framework for the Screening of Foreign Direct Investments into the Union. Before the regulation, there was no unified system that targeted or coordinated the investment screening policies of its member states. Under this change, a framework for information-sharing and investment reviewing procedures is being established. The regulation stipulates that the framework relates to screening measures on the basis of "security and public order" (European Parliament and the Council of the European Union, 2019, p. 2).

Notably, this regulation is non-binding, thus it is the responsibility of individual member states to implement an investment screening platform. Nevertheless, member states should notify the EU Commission on the introduction or extension of a screening mechanism, also regarding any transaction that has been reviewed, screened, or prohibited; reporting should also be conducted regarding any investment that took place within the territory of a member state (European Parliament and the Council of the European Union, 2019, p. 4).

At this stage, all but two EU member states have or are in the process of adopting FDI screening mechanisms. Akin to the Georgian context, the Czech Republic has recently initiated an FDI screening mechanism. The new Czech law introduces a tool for monitoring potentially risky capital inflows into the country, and it envisages restrictions placed on those investments that might be a security concern for Czech national interests (OECD, 2022, pp. 1-3).

As defined within this analysis, the core motive for adopting or tightening investment review procedures is to defend critical infrastructure and strategic assets. For instance, in the case of the Czech Republic, the sectors in which investments are mandatorily classified for review include military materials, dual use goods, critical infrastructure, and the administration of vital communication systems (OECD, 2022, p. 4). In many cases, it is specified that such screening mechanisms are to protect the citizenry from foreign influence, particularly Chinese or Russian influences for many Western countries. In the European Union, its recent measure of harnessing a union-wide FDI screening policy was motivated by growing hybrid threats to CI, those stemming from international players that have been detected "weaponizing their growing global economic footprint to achieve political objectives" (European Parliamentary Research Service , 2022, p. 1).

Moreover, the urgency of adopting such policy measures has been further exacerbated by Russia's full-scale war in Ukraine. The war has served to elevate the perception of Russia as both a) a hostile state actor and b) as a source of investment with high risk of damaging the security landscape in certain jurisdictions (UNCTAD, 2023, p. 7).

Among the measures targeted specifically towards Russia amid the war, those adopted by Italy, Canada, and the European Union are worth mentioning. According to the Policy Statement on Foreign Investment Review and the Ukraine Crisis, the Government of Canada declared that "an investment, regardless of its value, has ties, direct or indirect, to an individual or entity associated with, controlled by or subject to influence by the Russian state, this will support a finding by the

Minister that there are reasonable grounds to believe that the investment could be injurious to Canada's national security" (Government of Canada, 2022). Similarly, Italy corrected its existing screening mechanism in response to the war, and the country expanded the mandatory notification requirement for new legal entities carrying out activities in strategic sectors or when non-EU individuals hold more than 10% of the capital or voting rights (UNCTAD Investment Policy Monitor, 2022). Concurrently, the EU Commission urged member states to apply additional screening measures to control for the risk of any type of investment (beyond sanctions) in critical EU assets that "directly or indirectly relate to a person or entity associated with, controlled by or subject to influence by the Russian or Belarusian government" (European Commission, 2022, p. 1).

The existing investment screening mechanisms, particularly those emerging recently, share some common features:

- They target specific sectors of the economy that have strategic significance for the given nation. These sectors might differ from one country to another, but the list always covers sectors of critical infrastructure and critical information infrastructure (CII), and, if relevant, European critical infrastructure (ECI), which might also be applicable to other sectors beyond their criticality and depending on the scale of a transaction.
- They introduce a so-called "notification procedure", which, in some instances, is mandatory for parties that intend to invest in any of the pre-defined sectors (generally CI, CII, or ECI, as indicated above) with a high significance to national security. Beyond the obligatory nature of security, investors also have an opportunity to voluntarily notify the responsible agency to screen their transaction.
- The responsible agency (usually a dedicated evaluator or state entity) has the power of "calling-in" an investment that might be threating to national security, disregarding those belonging to the pre-defined sectors of CI, CII, or ECI. The power to call-in an investment for *ex officio* screening remains in the hands of the responsible agencies, retrospectively and for different timeframes (usually several years).
- As a result of the screening, the responsible authority might have the power to approve, suspend, or prohibit an investment. It might also have the discretion to impose sanctions, including, in certain cases, in the form of monetary and penitentiary penalties for non-compliant parties.

When reviewing FDI screening regimes, it is noteworthy that they are at times associated with controversial results. While, on the one hand, ensuring greater security, especially in relation to nation or cross-border CI or CII, investment screening regimes also significantly elevate the complexity of the host's regulatory framework for potential investors. For instance, in 2021, as Dechert LLP underscores, withdrawn merger and acquisition deals reached 700 bln. USD globally, surpassing the 2020, 2019, and the five-year average (Dechert LLP, 2022, p. 2). This occurred because regulatory uncertainty increases as screening regimes proliferate, which serves as a discouraging factor for re-investment or for launching new investments.

RECOMMENDATIONS

Considering the multi-dimensional evidence provided above, we can assume that Russia represents a threat actor in the context of Georgia. Russia's economic interests, including ownership stakes in the local economy, can be regarded as a hybrid tool to cause instability in Georgia and interfere in the stable, democratic, and sustainable development of the country.

When discounting the sectoral and infrastructural distribution of ownership, the threat test for Russian ownership in the Georgian economy highlights multiple warning signs. Russian ownership stakes in Georgian businesses should thus be regarded as posing threat considering the potential adversarial intentions of their owners, their capabilities, the relationships with the Russian state elite, alongside their track record as non-adherents to national and supranational regulations. Furthermore, the geopolitical context, driven by the ongoing war in Ukraine, provides additional warning signs; particularly in consideration of the linkages to the war of certain Russian oligarchs with former or existing ownership stakes in Georgia.

This research has identified multiple risk factors that relate to the general presence of foreign ownership in various national contexts. In Georgia, specifically, six distinct Russian ownership-related risks have been identified. These aspects were then assessed and ranked based on the expert judgment discerned during the research. This evidence reveals that all identified ownership-related risks have a high severity level, requiring a targeted, yet mindful policy response to mitigate the potential adverse impacts that might stem from their presence.

Foreign ownership itself should, per se, not be an alarming concern; especially in Georgia, which is ultimately reliant on foreign investments as a significant boost to economic stability and future prosperity. Nevertheless, in terms of Russian ownership, considering its scale and role in both critical sectors and in infrastructure, a dedicated policy regime might be required for effective regulation. In the absence of a strong institutional setup, it is probable that ownership positions will be exploited in order to undermine the normal course of life and increase harm during situations of heightened tension.

Consequently, it is crucial that the introduction of additional regulation in Georgia is based on state bureaucratic and fiscal capacities, as well as long-term security and foreign policy objectives, those which relate to Georgia's European and Euro-Atlantic Aspirations. Below we provide several recommendations targeted at mitigating such Russian ownership-related risks.

STUDY THE POTENTIAL IMPACT OF ADOPTING A FOREIGN DIRECT INVESTMENT (FDI) SCREENING MECHANISM

In order to adequately target ownership-related threats, it will be significant to modify the existing investment policy. One way to do this would be to implement an FDI screening mechanism, the functionalities of which are specified above. As discussed, there are several forms of implementation

for such a mechanism. Nevertheless, some common features can be traced across different jurisdictions.

For Georgia, there are several central considerations for designing an FDI screening tool. First, it is debatable whether such a mechanism should discriminatorily target investments from Russia (and countries that do not recognize Georgia's territorial integrity), or whether it should apply to all inward FDIs, regardless of their country of origin. Second, it should be subject to discussion whether all investments are screened, or if only those investments that target Georgian sectors and infrastructures of critical significance (i.e., the difference between cross-sectoral, sector-specific, and asset/infrastructural/entity-specific screening) should be checked. The third consideration relates to the potential volume of investment: arguably, it might be important to selectively screen only those inward FDIs that exceed a certain, pre-defined, monetary value. Such a value could be measured against different parameters, the most common being acquisition of a certain percentage (typically at least 10%) of shareholding or voting rights in a company. Lastly, it should be considered whether the screening authority has retrospective power to check *ex-post* potentially risky investments for national security.

Significantly, an FDI screening mechanism also comes with notable economic costs. As screening regimes proliferate, the regulatory landscape, in any national context, becomes more ambiguous, thus FDI inflow may slow; this could potentially have an adverse impact on short- to medium-term economic growth levels. Therefore, this report recommends an analysis of the potential costs and benefits of adopting an FDI screening regime, considering the diverse forms that this tool could take within different regulatory contexts (e.g., an *ex-ante* screening of Russian investments in critical sectors of the Georgian economy, through which an owner acquires at least 10% of shareholding rights).

Nevertheless, to operationalize this recommendation, it would be important to take steps in two additional directions, as specified below.

CONSIDERATION OF RUSSIAN OWNERSHIP-RELATED THREATS IN CONCEPTUAL NATIONAL SECURITY DOCUMENTS

There are several conceptual documents at the national level that target the field of security. For instance, the National Security Concept serves as the fundamental document for Georgia, reflecting its national interests and vision related to security. The National Security Concept puts forth key directions for Georgia's security, it also provides an overview of potential risks, threats, and challenges within the field. Besides the Concept, publication of the National Threats Assessment Document is envisaged, this would identify potential threats to Georgia's security, assess their scale, and the potential of actualization and impact. In addition, there are several further national strategies covering multiple directions, such as fighting corruption, money laundering, the disaster risk reduction strategy, etc. (National Security Council, 2023).

According to available information, Russian business-ownership related threats are not reviewed, evaluated, or specifically mentioned in any of these documents. For instance, while the National Security Concept does acknowledge the existential threat posed by Russian military presence in Georgia and the general hybrid threats stemming from Russia as potential risk to Georgian national security, the document does not stress the economic dimension of hybrid risks, nor is there a review of foreign business ownership as a potential threat to economic stability and national security. Equally, the National Threats Assessment document is not currently available, though it is important that it includes an evaluation of Russian business ownership-related risks.

During the process of designing an FDI screening mechanism, it is of utmost significance to base the scope of this instrument on a proper acknowledgment of the various risks related to Russia's business ownership. For instance, if, potentially, an FDI screening mechanism discriminatorily targets inward FDIs in critical sectors coming from Russia, it would be essential that the rationale of such a tool is built upon national fundamental security documents, such as the National Security Concept and the National Threats Assessment Document.

FOSTER ADOPTION OF CRITICAL INFRASTRUCTURAL REFORM THROUGH AN INCLUSIVE POLICY PROCESSES

Another significant step necessary to move forward the recommendation of employing an FDI screening mechanism is to foster the process around the adoption of critical infrastructural reform in Georgia. Fostering adoption of this reform, it is significant to have a nationwide agreement regarding the legal foundations for identifying and protecting Georgia's critical infrastructure. From the current standpoint, the country lacks a unified or consolidated definition of 'critical infrastructure' and of the related sectors; rather, the available definitions are scattered across different regulatory frameworks. This would potentially impact creating an FDI screening tool that targets inward investments in critical infrastructure and in vital sectors. Nevertheless, screening inward FDIs in critical infrastructure, as noted above, is the most common global practice shared by different countries to have adopted some form of investment review procedure.

Significantly, Georgia is already in the process of adopting its Critical Infrastructure reform, the process being led by the National Security Council. However, from the current perspective, the process seems to be progressing slowly. Within this reform, an FDI screening mechanism within critical infrastructure is envisaged in order to ensure local CI protection. Therefore, implementing this reform would effectively translate into operationalization of our main recommendation – to mindfully consider the establishment of some form of investment review procedure in the country.

Additionally, there can be differing views regarding the scope of this reform, thus all necessary professional and expert opinions should be considered when promoting policy change. As such, it becomes significant to ensure an inclusive policy process during the adoption of critical infrastructural reform. Thus, to efficiently target the essential sectors in the Georgian economy and

to ensure trust regarding any implemented policy change, it is important to promote stakeholder engagement during reform implementation.

Lastly, policy changes that have been recommended through this research project have to be specifically assessed against the costs that they might produce. For instance, implementing an investment review procedure might necessitate bureaucratic and intellectual capacities that exceed the available resources or the potential benefits stemming from policy change. Accordingly, additional examination is needed regarding the advantages and appropriateness of all recommended actions.

CONCLUSION

In summation, based on a literature review and qualitative expert interviews, this study examined the risks and threats associated with Russian business ownership within the Georgian economy. The given analysis is based on the sectoral findings of the Institute for Development of Freedom of Information (IDFI), and covers the current extent of Russian ownership in eight sectors of the economy, namely: electricity, communications, oil and gas, mining and mineral waters, tourism, construction, banking and transportation. The findings reveal significant Russian influence in the electricity sector, noticeable influence in the oil and gas sector, and moderate influence in the communications and in the mining and mineral waters sectors. Whereas low to non-existent Russian ownership-related influence can be traced within the remaining four sectors.

This study contextualizes the research across several directions. First, it argues that Russia acts a global threat actor, and it poses existential security challenges to Georgia; considering Russian military occupation of 20% of internationally recognized Georgian territory, borderization and creeping occupation, alongside the unconventional hybrid tools utilized to gain additional leverage as the country pursues its Euro-Atlantic aspirations. Furthermore, the study has demonstrated that, among hybrid tactics, business ownership by hostile state actors represents a significant hybrid tool. Such a mechanism can be exploited under several means, including to gain political leverage, to manipulate economic instruments, to gain access to sensitive information, or to plan cyberattacks. Lastly, the analysis particularly emphasized the threats associated with foreign ownership within critical infrastructure and vital sectors due to the unique vulnerabilities that such infrastructures face, such as their interdependency, wide accessibility, societal and symbolic value, among other issues.

In the context of Georgia, besides Russia's history of hostility and the hybrid nature of foreign ownership, Russian ownership or Russian linkages can be found within critical infrastructural sectors, such as energy, communications, and in ports (e.g., the Poti oil terminal). This serves to further exacerbate Georgia's vulnerability towards the potential risks and threats that might arise from Russian business ownership.

The study subsequently named six distinct risks that can be associated with Russian business ownership in Georgia. Primarily, considering the intertwinement of interests among Russian political and business elites, we have argued that ownership might grant Russia additional political influence over Georgia. Second, we indicate the risk of corruption (e.g., tax evasion, money laundering, revolving door incidents, exploiting the public procurement system, etc.) as a significant threat considering previous Russian acts of corruption in Georgia and the neighboring countries. Third, the analysis demonstrates that economic dependency, or "sphere capture," is yet another threat that might create a risk of economic manipulation, such as price manipulation. Furthermore, espionage, either commercial, political, or related to personal information, is regarded as an additional risk associated with Russian ownership, particularly considering the empirical evidence of the demonstrated ties between Russian business operators (e.g., Yandex Go) and

Russian intelligence agencies. Furthermore, we identify sabotage as another hazard with the potential of actualization through Russian business ownership. Lastly, the study emphasizes the risk of sanctioning and sanction evasion, namely in consideration of the existing global sanction regimes targeting Russia and Russia-affiliated businesses.

The conducted risk assessment exercise revealed a high severity level for each aspect identified. Nevertheless, compared to other factors, the severity in political influence, sanctioning and sanction evasion, as well as economic dependency and manipulation increases noticeably with Russian business ownership. Significantly, the latter risk of economic dependence and manipulation is particularly elevated with the factor of Russian ownership.

From the various risk mitigating measures, the study has particularly stressed foreign direct investment screening mechanisms, which are currently being adopted by more and more economies globally. Although applications of this tool differ, the existing FDI review procedures share certain common features, such as targeting pre-defined sectors with high security concerns (e.g., critical infrastructural sectors); introducing the so-called "notification procedure," making it mandatory for potential investors to notify a screening agency regarding transactions; or having retrospective power as well as the power to suspend or terminate a transaction if security concerns are detected.

In the local context, we recommended a further study of the potential impact of introducing an FDI screening mechanism. Implementation of this tool should be checked against its potential economic impacts, state bureaucratic capabilities, and the overall regulatory desirability of introducing such a policy change. In order to operationalize the aforementioned recommendation, however, the study indicates the necessary to i) include an overview of Russian ownership-related risks in national conceptual security documents of; and ii) foster the adoption of critical infrastructural reform in Georgia through inclusive policy processes.

As a final note, it should be stressed that the presence of Russian business ownership in the Georgian economy is just a small piece of the total economic leverage that Russia has over the country. In order to adequately assess the scope of the problem, it is therefore important to examine how concerning the overall economic dependency on Russia has become, including the factor of Russian business ownership in the economy. Moreover, beyond Georgia's declared mission of approximating with the Euro-Atlantic space, new state actors are also emerging as potential economic and strategic partners (e.g., China). It will consequently be significant, if not relevant, to understand the international practice of protecting national security from potentially malign influences (e.g., ownership-related influences), associated with the excessive presence of these actors as economic interest groups that gain notable form of local control.

GLOSSARY

Hybrid threats – hybrid threats combine both military and non-military, conventional and non-conventional means to achieve strategic goals. These might include disinformation campaigns, cyber-attacks or utilizing regular armed forces.

Critical Infrastructure (CI) – infrastructures are critical if their degradation/incapacitation would paralyze normal course of life and significantly diminish safety of citizens. Critical infrastructure might include railways, electric power networks, telecommunications and port facilities, dams, gas pipelines, etc.

Critical Information Infrastructure (CII) – assets, networks, processes, either virtual or real, which are part of information and communication systems, and which are so important that their degradation or incapacitation would paralyze normal course of life and significantly diminish safety of citizens.

State capture – domination of state institutions by ruling elite or private interest groups, which manipulate policy formation and significantly influence both political and economic rules of the game.

Espionage – practice of intelligence gathering to obtain different types of information (e.g. economic, political, personal, security-related), which will be unlawfully transferred to another organization/state.

Cyber-espionage – practice of espionage utilizing computer/digital networks.

Sabotage – intentional damage or destruction of equipment, weapons, networks or buildings to weaken an enemy or competitor.

Cyber-sabotage – practice of sabotage utilizing computer/digital networks.

Essential services – essential are those services that meet basic needs of the public. For instance, these services include provision of water, food, gas, electricity, etc., that are essential to preserve life.

Proxy tools – term "proxy" is usually referred to those tools or strategies that are utilized by malign state actors (e.g. Russia) to mask their real intentions.

Supply chain – term refers to systems and networks which turn raw materials into finished, ready-to-sale products.

Dual-use technologies – technologies that can have both civilian and military applications. Examples of dual-use technologies might include drones, computers, Artificial Intelligence (AI), electronics, etc.

Cascading effect – reaction in an interconnected network, when an event in one system has a negative impact on other, related systems.

Merger and Acquisition (M&A) – these terms refer to joining of two companies. However, merger relate to the process when two separate companies combine forces to create one entity, while acquisition relates to the process of takeover of one small company by another, larger player.

Borderization – erecting the demarcation line in the zone of conflict. The process of installing artificial border signs, fences, barbed-wires to create a so-called "occupation line".

Notification procedure – a mandatory procedure to go through for potentially risky investments in different jurisdictions with investment screening mechanisms in place.

Retrospective power – a power of the screening authority to check security of those investment transactions that have already been made.

REFERENCES

Amnesty International. (2022, October). *Ukraine: Russian attacks on critical energy infrastructure amount to war crimes.* Retrieved from amnesty.org: https://www.amnesty.org/en/latest/news/2022/10/ukraine-russian-attacks-on-critical-energy-infrastructure-amount-to-war-crimes/

ARKA News Agency. (2023, February). *Armenia's imports of Russian natural gas in 2022 grew by 6.1% to about 2.6 billion cubic meters -Gazprom-Armenia.* Retrieved from arka.am: https://arka.am/en/news/business/armenia_s_imports_of_russian_natural_gas_in_2022_grew_by_6_1_to_about_2_6_billion_cubic_meters_gazpr/

BMG. (2023). *Yandex to Share Taxi Data in Georgia, Israel, Kazakhstan and 17 Other Countries with FSB.* Retrieved from Business Media Group: https://bm.ge/en/news/yandex-to-share-taxi-data-in-israel-georgia-kazakhstan-and-17-other-countries-with-fsb

Conley, H. A., Mina, J., Stefanov, R., & Vladimirov, M. (2016). *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe.* Retrieved from Center for Strategic and International Studies: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf

Cyber and Infrastructure Security Centre (CISC). (2023). Retrieved from Critical Infrastracture Resilience Stratagey: https://www.cisc.gov.au/resources-contact-information-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

Dechert LLP. (2022, May). *The Evolving Global Foreign Direct Investment and National Security Review Landscape.* Retrieved from dechert.com: https://www.dechert.com/knowledge/publication/the-evolving-global-foreign-direct-investment-and-national-secur.html

Department of Public Safety and Emergency Preparedness. (2023). *Public Safety Canada.* Retrieved from Canada's Critical Infrastructure: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

European Commission. (2022). *Guidance to the Member States concerning foreign direct investment from Russia and Belarus in view of the military aggression against Ukraine and the restrictive measures laid down in recent Council Regulations on sanctions.* Retrieved from https://eur-lex.europa.eu/: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XC0406(08)

European Parliament. (2021). *European critical infrastructure Revision of Directive 2008/114/EC.* Retrieved from europarl.europe.eu: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

European Parliament and the Council of the European Union. (2019). *REGULATION (EU) 2019/452 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March of 2019 on establishing a framework for the screening of foreign direct investments into the Union* . Retrieved from https://eur-lex.europa.eu/: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452

European Parliamentary Research Service . (2022, December). *Question time: Protecting strategic infrastructure against Chinese influence* . Retrieved from European Parliamentary Research Service (EPRS): https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739248/EPRS_ATA(2022)739248_EN.pdf

Fekete, A. (2011). *Common Criteria for the Assessment of Critical Infrastructures.* Retrieved from link.springer.com: https://link.springer.com/content/pdf/10.1007/s13753-011-0002-y.pdf

FOI. (2022, December). *Russian Investments and Financial Interests in Sweden.* Retrieved from Swedish Defense Research Agency (FOI): https://www.foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5377--SE

German Federal Office for Information Security . (n.d.). *What are Critical Infrastructures?* Retrieved from Federal Office for Information Security: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html#:~:text=Critical%20infrastructures%20(%20KRITIS%20)%20are%20organisations,security%20or%20other%2

Governance Monitoring Center . (2023, July). *Georgia and Western Sanctions on Russia.* Retrieved from Governance Monitoring Center (GMC): https://drive.google.com/file/d/1AluwUOidIJ2Q4BsvBuygUeSKGDMEX5y8/view?fbclid=IwAR39wKS2PiyW_PCR2it-mBFoa8EDHq1FGbk3_jrz0qVWniiDM06RzC4ql5Y

Government of Canada. (2022). *Policy Statement on Foreign Investment Review and the Ukraine Crisis.* Retrieved from https://ised-isde.canada.ca/: https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/policy-statement-foreign-investment-review-and-ukraine-crisis

Herreraa, L.-C., & Maennel, O. (2019). *A comprehensive instrument for identifying critical information infrastcructure services.* Retrieved from pdf.sciencedirectassets.com: https://pdf.sciencedirectassets.com/277415/1-s2.0-S1874548219X00037/1-s2.0-S1874548217300422/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEDwaCXVzLWVhc3QtMSJHMEUCIHfafqB%2B0nq8DbLzc4A68OhWAzxvHjF4A5EsD5N3mpDBAiEAw3w5ns8FsJuoJBx56%2B0fQnIyDBFNpJqqBfFqYB6A

Institute for Development of Freedom of Information (IDFI). (2022, Nivember). *Russian Capital and Russian Connection in Georgian Business.* Retrieved from idfi.ge: https://idfi.ge/public/upload/Analysis/EN_IDFI_Report.pdf

Institute for Development of Freedom of Information (IDFI). (2022). *Russian Capital in Georgian Business: Primary Study of Communications, Banking, Mining and Mineral Waters Sectors.* Retrieved from idfi.ge: https://docs.google.com/viewerng/viewer?url=https://idfi.ge/public/upload/Analysis/IDFI+Report_Final_ENG_compress.pdf

Institute for Development of Freedom of Information (IDFI). (2023, June). *Russian Capital and Russian Connections in Georgian Business.* Retrieved from idfi.ge: https://idfi.ge/public/upload/Analysis/Russian%20capital%20and%20Russian%20connections%20in%20Georgian%20business.pdf

IWPR. (2022). *Georgia Nationalises Iconic Mineral Water Due to Russian Sanctions.* Retrieved from iwpr.net: https://iwpr.net/global-voices/georgia-nationalises-iconic-mineral-water-due-russian-sanctions

Izuakor, C., & White, R. (2016). *Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis.* Retrieved from links.springer.com: https://link.springer.com/chapter/10.1007/978-3-319-48737-3_2

Le Monde. (2022, November). *The Russian spy couple caught in the 'burbs: In Sweden, 'The Americans' plays out in real life.* Retrieved from lemonde.fr: https://www.lemonde.fr/en/international/article/2022/11/28/a-russian-spy-couple-caught-in-the-burbs-in-sweden-the-americans-plays-out-in-real-life_6005900_4.html

Mckew, M. K. (2017, October). *The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare. And it's probably being used on you.* Retrieved from Politico.com: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/

Mishcon de Reya. (2022). *The National Security and Investment Act: protecting UK assets and infrastructure.* Retrieved from mishcon.com: https://www.mishcon.com/the-national-security-and-investment-act-protecting-uk-assets-and-infrastructure

Mitrevska, M., Mileski, T., & Mikac, R. (2018). *Critical Infrastructure: Concept and Security Challenges.* Retrieved from Friedrich-Ebert-Stiftung Skopje: https://skopje.fes.de/fileadmin/user_upload/images/critical/Critical_Infrastructure_EN_-_web.pdf

National Endowment for Democracy. (2019). *War by Other Means, Kremlins Energy Policy as a Channel of Influence: Comparative case Studies from Ukraine, Moldova, Romania and*

Hungary. Retrieved from National Endowment for Democracy: https://expertforum.ro/en/kremlins-energy-policy-as-a-channel-of-influence-a-comparative-assessment/

National Protective Security Authority . (2023, April). *Critical National Infrastructure.* Retrieved from National Protective Security Authority : https://www.npsa.gov.uk/critical-national-infrastructure-0

National Security Council. (2023). *nsc.gov.ge.* Retrieved from National Security Council: https://nsc.gov.ge/en/CONCEPTUAL-DOCUMENTS/National-Strategies-in-security-fiel

OECD. (2020). *Investment screening in times of COVID-19 and beyond.* Retrieved from Organization for Economic Co-operation and Development (OECD): https://www.oecd.org/coronavirus/policy-responses/investment-screening-in-times-of-covid-19-and-beyond-aa60af47/

OECD. (2022). *Investment policy related to national security: Notification by Czech Republic.* Retrieved from Organization for Economic Co-operation and Development (OECD): https://one.oecd.org/document/DAF/INV/RD(2023)1/en/pdf

Park, D., & Walstrom, M. (2017, October). *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.* Retrieved from jsis.washington.edu: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Polinpapilinho, K., & Patrick, H. (2013). *Systemic determination of infrastructure criticality.* Retrieved from ideas.rpec.org: https://ideas.repec.org/a/ids/ijcist/v9y2013i3p211-225.html

Politico. (2022, December). *Russian oligarch Mikhail Fridman detained on money-laundering suspicions: Report.* Retrieved from Politico.com: https://www.politico.eu/article/2380338/

RFERL. (2020). *Russian Armenian Dispute over Railway 'Settled'.* Retrieved from https://www.azatutyun.am/a/30819063.html

RFERL. (2023, May). *Sanctioned Billionaire Fridman Linked To Insurance On Russian Military Vehicles Used In Ukraine.* Retrieved from RFERL: https://www.rferl.org/a/ukraine-fridman-russian-military-vehicles-schemes-scandal/32404641.html

RTVI. (2019). *Russia is preparing to terminate the service of the Armenian railway ahead of schedule. This is connected with the criminal case against the daughter of Russian Railways.* Retrieved from RTVI.com: https://rtvi.com/stories/rossia-gotovitsya-dosrochno-prekratit-obsluzhivanie-zheleznoy-dorogi-armenii/

Terzyan, A. (2018). *The anatomy of Russia's grip on Armenia: Bound to Persist?* Retrieved from econstor.eu: https://www.econstor.eu/bitstream/10419/198543/1/ceswp-v10-i2-p234-250.pdf

The Council of the European Union. (2008, December 8). *COUNCIL DIRECTIVE 2008/114/EC.* Retrieved from on the identification and designation of European critical infrastructures and the assessment of the: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

The New York Times. (2023, June). *Why the Evidence Suggests Russia Blew Up the Kakhovka Dam.* Retrieved from nytimes.com: https://www.nytimes.com/interactive/2023/06/16/world/europe/ukraine-kakhovka-dam-collapse.html

Transparency International Georgia. (2023, March). *Russian Ties and Corruption Risks of an Electricity Importer Company.* Retrieved from www.transparency.ge: https://transparency.ge/en/blog/russian-ties-and-corruption-risks-electricity-importer-company

U.S. Congress. (2001). *USA Patriot Act of 2001.* Retrieved from Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

UNCTAD. (2023, February). *The Evolution of FDI screening mechanisms - key trends and features.* Retrieved from United Nations Conference on Trade and Development (UNCTAD) - Investment Policy Monitor: https://investmentpolicy.unctad.org/publications/1279/the-evolution-of-fdi-screening-mechanisms---key-trends-and-features

UNCTAD Investment Policy Monitor. (2022). *Italy approves further changes to the FDI screening regime.* Retrieved from UNCTAD Investment Policy Monitor: https://investmentpolicy.unctad.org/investment-policy-monitor/measures/3993/italy-approves-further-changes-to-the-fdi-screening-regime-

ANNEXES

Annex 1: Suspicious incidents in 2022 potentially involving Russia

In March, multiple airplanes in Finland experienced abnormal GPS disruptions, leading to the inability to land at the Savonlinna airport, situated close to the Russian border. According to Jukka Savolainen from the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), these occurrences were likely connected to Russia's employment of hybrid tactics. While it remains uncertain whether these disruptions were a deliberate attack or an unintentional outcome of Russia's military exercises, Savolainen stressed the importance of Finland being prepared for further interference.

In August, authorities in Estonia announced that the nation had encountered its most significant cyberattack since 2007. During this large-scale attack, various Estonian websites, including those of the parliament, newspapers, banks, and government ministries, were specifically targeted (Euronews, 2022). The pro-Russia hacker group known as Killnet claimed responsibility for the attack, asserting that it had successfully impeded access to more than 200 state and private institutions. However, Estonian officials downplayed the impact of the event, describing it as causing only minor disruptions.

In October, there was a notable disruption to a railway system in northern Germany when crucial communication cables were deliberately severed at two distinct locations (France 24, 2022). As a result, train operations were halted for a duration of three hours, leading to significant chaos and inconvenience for thousands of passengers. German Transport Minister Volker Wissing characterized this incident as an act of "sabotage," emphasizing its deliberate and malicious nature, with clear indications of premeditation. While not directly attributing blame to Russia, Wissing acknowledged that the involvement of a foreign power could not be dismissed. On the other hand, Anton Hofreiter, a Green party MP, more directly implicated the Kremlin, suggesting that the incident might have been intended as a warning to Germany due to its support for Ukraine. Despite these speculations, no concrete evidence has been presented to substantiate Moscow's responsibility for the incident.

Also in October, there were simultaneous incidents of internet cable cutting at three distinct locations in the southern part of France, resulting in severe disruptions to both internet and phone services. The internet service provider Free described the occurrence as an act of vandalism on their fiber infrastructure (Al Jazeera, 2023). Notably, a similar incident had taken place in April when intentional cuts to internet cables occurred at multiple locations near Paris, leading to a widespread internet blackout affecting thousands of people (Wired, 2023). Nicolas Guillaume, the CEO of one of the affected providers, argued that the cables were deliberately cut in a manner that caused substantial damage, necessitating significant time for repairs, suggesting that it was "the work of professionals".

In February, Dutch authorities disclosed that several hospitals across Europe had fallen victim to targeted attacks by the group known as Killnet. However, they stated that the impact of these attacks was relatively limited (Euronews, 2023). The nature of the attacks appeared to focus on countries that had shown strong support for Ukraine, including the United Kingdom, Germany, Poland, and the United States.

Source: *Pillai, H. (2023, April). Protecting Europe's critical infrastructure from Russian hybrid threats.*

Annex 2: Instances in which Russia used its energy leverage against Georgia

Year	Event	Geopolitical Rationale	Further Rationale
2004 - 2006	Gazprom demanded a nearly 500 percent price increase, from $50 to $235 per thousand cubic meters	Applying energy sanctions to the 'disobedient' Georgian leader, the newly elected pro-western president Mikheil Saakashvili	A 'normal' price increase, designed to bring Georgia in line with prices charged to Moscow's Western European purchasers, which the Kremlin described as the "world market price"
2006 Winter	Cut off from the Russian energy supply during a very cold winter. Sabotage of the two alternative branches of the main gas pipeline and blowing up an electricity import transmission tower left the Georgian population without gas for two weeks	To create instability in the country	Russia announced that both the main gas lines to Georgia had been cut by bomb blasts, allegedly by Chechen separatists
2008	Attack on the Baku-Tbilisi-Ceyhan (BTC) pipeline – disrupting oil transportation for 14 days	Undermining the reliability of the southern export route for Caspian gas	Russia denied any connection with the incident. However, according to Bloomberg's seven-year investigation, the BTC pipeline was destroyed by hackers who used ultra-modern computer technologies and were supported by Russian Special Services
2016	Gazprom-Export demanded a change to the gas transit agreement, switching from in-kind payments to monetary compensation	Unclear	Using the principles of International Legal Framework, which forbids in-kind payment
2019	Increase gas transit fee (monetary compensation)	Unclear	Unclear

Source: *War by Other Means, Kremlin's Policy as a channel of Influence: Comparative Case Studies from Ukraine, Moldova, Georgia, Romania, and Hungary*

Annex 3: Definitions of "Critical Infrastructure" in the European Union, the United States, Australia, Germany, the United Kingdom and Canada

COUNTRY/ JURISDICTION	DEFINITION
European Union	"European Critical Infrastructure (ECI) means critical infrastructure located in member states the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria" (The Council of the European Union, 2008).
The United States	"The term ''critical infrastructure'' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (U.S. Congress, 2001).
Australia	"Critical Infrastructure is defined as those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of Australia as a nation or its states or territories, or affect Australia's ability to conduct national defense and ensure national security" (Cyber and Infrastructure Security Centre (CISC), 2023).
Germany	"Critical Infrastructures are organizations and facilities of major importance for society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order, safety and security or other dramatic consequences" (German Federal Office for Information Security, 2023).
United Kingdom	"Assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them, the loss or compromise of which could result in: a) major detrimental impact on the essential services or b) significant impact on national security, national defense, or the functioning of the state" (National Protective Security Authority , 2023).
Canada	"Critical infrastructure (CI) refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence" (Department of Public Safety and Emergency Preparedness, 2023).

Annex 4: Risk Assessment Tools Utilized Across Different Countries

National Security Reviews	Many countries have established national security review mechanisms to assess foreign investments and acquisitions that may have implications for national security. These reviews are conducted by governmental agencies responsible for national security, such as the intelligence community, defense agencies, or specialized investment review bodies. They examine the potential risks posed by foreign ownership and determine whether mitigation measures or restrictions are necessary.
Sector-specific Assessments	Governments often conduct sector-specific assessments to evaluate the national security implications of foreign ownership in critical sectors. These assessments focus on industries such as defense, telecommunications, energy, transportation, and technology, where foreign ownership may pose significant risks. They consider factors such as the criticality of the sector, technological advancements, supply chain vulnerabilities, and the potential impact on national security capabilities.
Risk-based Approaches	States may adopt a risk-based approach to assess foreign ownership risks. This involves evaluating factors such as the country of origin, the nature of the investment, the level of control or influence the foreign entity would have, and the potential consequences of foreign ownership. Risk assessments may consider geopolitical considerations, the presence of state-owned enterprises, previous behavior of the foreign entity, and the regulatory environment in the country of origin.
Intelligence Gathering and Analysis	Governments rely on intelligence agencies to gather and analyze information regarding foreign entities seeking ownership stakes in critical industries. Intelligence assessments provide insights into the intentions, capabilities, and potential risks associated with foreign owners. These assessments often involve assessing the geopolitical context, potential linkages to state actors, and the likelihood of adverse actions by foreign owners.
Collaboration with Allies and International Partners	States may collaborate with allied countries and international partners to exchange information, share best practices, and collectively assess the risks associated with foreign ownership. These collaborations can enhance the understanding of global trends, emerging risks, and potential threats posed by foreign investors.
Legislative and Regulatory Frameworks	Governments establish legislative and regulatory frameworks to define the parameters within which foreign investments are evaluated for potential risks. These frameworks may include specific laws, regulations, and guidelines that provide clarity on the assessment process, criteria for evaluating risk, and mechanisms for imposing mitigation measures or restrictions on foreign ownership.

Annex 5: List of Interviewed/Surveyed Experts

Expert	Organization
Anton Vatcharadze	Institute for Development of Freedom of Information (IDFI)
Giorgi Goguadze	Georgian Center for Security and Development (GCSD)
Murman Margvelashvili	World Experience for Georgia (WEG)
Eka Akobia	Caucasus University
Irakli Porchkhidze	Georgian Institute for Strategic Studies
Davit Sikharulidze	Security Expert
Batu Kutelia	Security Expert
Gigi Gigiadze	Economic Policy Research Center (EPRC)
Giorgi Muchaidze	Atlantic Council of Georgia
Tazo Kupreishvili	Netgazeti