U4 ANTI-CORRUPTION RESOURCE CENTRE

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

U4 HELPDESK ANSWER 2026: 5

Illicit finance, financial secrecy and state threats

Sam Parrett-Jung

Reviewed by

Jamie Bergin, Vincent Freigang, Katherine Wilkins and Buren Mandakhbileg (TI)

Rosa Loureiro-Revilla (U4)

Illicit finance vulnerabilities can be exploited by state-linked actors to conduct a range of threat activities, such as access to strategic sectors, cyberthreat operations, corruption and foreign political interference. Notably, opaque ownership or shell companies are used to obscure control, move value and reduce attribution linked to threat activities. Experts recommend strengthening beneficial ownership transparency, verification and information sharing, while cautioning against over-securitised responses that risk selective enforcement or undermine longer term institutional reform.

CMI CHR. MICHELSEN INSTITUTE

U4 Helpdesk Answers are tailor-made research briefings compiled in ten working days. The U4 Helpdesk is a free research service run in collaboration with Transparency International.

helpdesk@u4.no

Related U4 reading

Illicit finance and national security (2021)

Illicit financial flows, fragility and conflict (2024)

Links between illicit financial flows and peace and security (2014)

How to cite

Parrett-Jung, S. 2026. Illicit finance, financial secrecy and state threats. Bergen: Transparency International and U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute (U4 Helpdesk Answer 2026: 5)

Published

2 April 2026

Keywords

National security risks, illicit finance, state threats

Query

Please conduct a literature review of the available empirical evidence on the relationship between state-threat linked national security risks and illicit finance, particularly issues related to financial secrecy and corporate transparency, in a global context.

Main points

- Existing literature links illicit finance vulnerabilities to state threats primarily through documented mechanisms of concealment, including the use of shell companies, nominee arrangements and layered ownership structures.
- Additionally, the exploitation of the pseudonymity and other vulnerabilities of virtual assets, such as cryptocurrencies, is an emerging area of concern.
- Although it is not always possible to clearly identify national security implications, case evidence shows that opaque corporate and financial structures are used for the purposes of access to strategic sectors, cyberthreats, corruption and forms of foreign political interference such as covert political finance.
- Financial secrecy vehicles are also exploited as part of sanctions evasion schemes, which aim to hinder countermeasures designed to address state threats, including proliferation.
- The literature emphasises that policy responses tend to focus on improving beneficial ownership transparency, verification and information sharing, while cautioning against over-securitisation and selective enforcement, which may negatively affect multilateral efforts to counter illicit finance.
- While there is strong documentation of how structures used to obscure company and asset ownership are used in state-linked activity, there is less evidence – particularly in the form of robust quantitative, longitudinal studies – that can test whether changes in the use of financial secrecy are associated with measurable security relevant outcomes.

Contents

Introduction

Illicit finance and financial secrecy are increasingly being discussed in reference to national security issues (Kiepe 2021), primarily because obscure ownership or control over financial flows can facilitate state threats such as the penetration of, or access to, strategic and sensitive sectors (Kiepe 2021), cyberthreats (Bernhard et al. 2024), covert foreign political finance (Bak 2021), strategic corruption (Kassa and Guy 2025) and sanctions evasion schemes that hinder countermeasures designed to address state threats (FATF 2025). This reflects a wider policy push to treat weaknesses in corporate transparency and financial systems not only as corruption or compliance problems (see Transparency International 2022a) but also as vulnerabilities that can be exploited for state threats (see Kiepe 2021).

This Helpdesk Answer explores literature concerning the relationship between illicit finance vulnerabilities and state threats that generate national security risks (henceforth state threats), specifically the ways in which financial secrecy or a lack of transparency over the ownership of companies, trusts and other assets are used by states to threaten another country's national security. It documents what the existing literature and case evidence can reliably show about these links and maps key mechanisms through which financial secrecy can create or increase security risks.

Framework and caveats

This answer is broken into different threat areas. For each of these the review links: i) the relevant illicit finance vulnerabilities; ii) how those vulnerabilities are exploited in practice; and iii) the security relevant effects they enable. In many instances, the available evidence can robustly show that anonymous companies and opaque structures are used for state threats, but it usually does not allow for clear attribution of downstream national security outcomes.

There is a lack of longitudinal, regression based studies, like those common in the wider anti-corruption literature, testing, for example, whether jurisdictions with weaker beneficial ownership transparency experience worse security relevant outcomes or whether improvements in transparency lead to identifiable changes over time (Open Ownership 2022). These gaps are partly driven by data constraints, including uneven disclosure rules (see OECD and IDB 2024), limited verification (see World Bank 2023), and the use of secrecy jurisdictions and cross-border structures that obscure ultimate beneficial owners (see Garcia-Bernardo et al. 2017). This paper therefore relies primarily on case evidence to map financial secrecy mechanisms in

practice. However, these cases are illustrative rather than representative and cannot provide definitive conclusions on the relationship between financial secrecy and national security outcomes.

States are increasingly incorporating illicit finance strategies into their national security objectives (see Home Office 2026; US Department of the Treasury 2024). This comes largely from the understanding that illicit finance plays a crucial role in driving national security threats by enabling state actors, criminal networks and corrupt elites to pose systemic risks to governance, markets and public trust. Existing literature does not provide a conclusive view on the potential benefits and drawbacks of framing illicit finance issues through a national security lens but rather highlights that such framing can generate both legitimising effects for countermeasures and feedback loops that may worsen security problems over time (Nizerro 2024; Otokuya 2024; Baysal 2020; Lenz-Raymann 2014).

Box 1 – Framing concepts as national security threats

Nizerro (2024) highlights that framing concepts as national security threats (securitisation) can carry significant risks. In such cases, concepts may be placed on security agendas and considered as issues that require urgent policy responses or become framed in a biased manner. The literature has identified some key "unintended consequences" that can arise from securitisation:

- **Politicisation and selective enforcement**: security framing can concentrate attention on geopolitically salient actors or cases, leading to uneven enforcement and distorted threat perceptions, while other risks or domestic enablers receive less attention (Nizerro 2024; Baysal 2020).
- **Prioritise short-term responses rather than the sustained structural reforms**: securitisation may favour high-visibility, rapid tools such as sanctions or asset freezes, diverting attention and resources away from longer term institutional investments (Nizerro 2024).[1] Securitisation may also be operationalised through intelligence and espionage practices that translate threat narratives into action and legitimise extraordinary state measures; in cyber contexts, these practices can heighten risks of misperception, escalation and eroded trust, reinforcing the importance of clearer legal–normative constraints and "intelligence diplomacy" to mitigate destabilising effects (Azmi 2025: 134).

[1] For example, Nizerro (2024: 75) argues the UK response following Russia's 2022 invasion of Ukraine illustrates how security framing concentrated attention on oligarchs and asset freezes, resulting in an "oversimplification" of what was required as an effective response.

- **Erosion of democratic processes and civil liberties**: the normalisation of exceptional measures can weaken legal safeguards, reduce oversight and justify actions that risk infringing on rights or undermining the rule of law (Nizerro 2024; Otukoya 2024). For example, Otukoya (2024) highlights how a securitisation narrative can dehumanise certain groups, portraying them as inherent threats.
- **Exclusion of relevant stakeholders**: national security framing can increase secrecy and limit participation by civil society, regulators and other non-security actors (Nizerro 2024). Baysal (2020) highlights the top-down framework of securitisation that facilitates this process.

With this in mind, it is possible that the literature that explores illicit finance and state threats may reflect a selection or partisan bias where political and institutional attention is concentrated on geopolitically salient actors.

Definitions

Illicit finance: there is no single agreed-upon definition of the term illicit finance, but definitions exist for the closely related concept of illicit financial flows (IFFs). According to the IMF (2023), IFFs refers to "the movement of money across borders that is illegal in its source (e.g. corruption, smuggling), its transfer (e.g. tax evasion), or its use (e.g. terrorist financing)". In other words, illicit finance concerns money that is shaped by where it originates, how it is moved and/or what it is used for. Notably, what constitutes illicit and licit activity is often unclear since actions that are widely viewed as harmful may still be lawful, and the same funds can be used for both legal and illegal means (Bak 2021).

Illicit finance vulnerability: in this context, vulnerability can be defined as "a characteristic or specific weakness that renders an organisation or asset open to exploitation by a given threat or susceptible to a given hazard" (Injac 2016). In many instances, illicit finance vulnerabilities can be created or exacerbated through corruption (see Reed and Fontana 2011).

This paper focuses specifically on financial secrecy. In this context, these terms primarily refer to the absence or insufficiency of beneficial ownership transparency for locally registered companies (see Transparency International 2022a) or trusts (see Goodrich and Mollat 2025), as well as to opaque asset ownership, such as when property or other assets are anonymously held (see Brimbeuf et al. 2023) or layered legal vehicles that obscure the individuals or state-linked actors exercising control (see FATF and Egmont Group 2018).

National security: national security is a highly contested term in the literature, where a range of narrow to wide definitions have been adopted. For the purposes of this paper, a wider definition is used, and national security is understood as the "protection and safety of the political, economic and other interests and values of the state" (Injac 2016).

Foreign political interference: foreign interference is also a contested term in the literature (Berzina and Soula 2020; Bressanelli 2021). Berzina and Soula (2020) distinguish foreign interference from legitimate inter-state practices such as diplomacy by its marked malicious intent and lack of transparency. Similarly, the Government of Canada (n.d.) distinguishes foreign interference from influence, where "foreign partners generally use legitimate, legal and transparent means to advocate their interests" (Government of Canada n.d.). In contrast, foreign political interference involves "clandestine, deceptive, manipulative or personally threatening actions by foreign governments, or those acting on their behalf, to manipulate Canada's policies, elections or public opinion" (Government of Canada n.d.). These actions range from covertly influencing elections to spreading disinformation to influence public opinion. This paper adopts a similar understanding of foreign political interference, covering threats that arise both within and outside electoral cycles and are directed at political figures and the public.

Covert political finance: for the purposes of this paper, covert foreign political finance is understood as a form of political interference and will follow Rudolph and Morley's (2020) definition: "the funding of foreign political parties, candidates, campaigns, well-connected elites or politically influential groups, often through non-transparent structures designed to obfuscate ties to a nation state or its proxies".

State threats: RUSI (n.d.) uses the term state threats for hostile activity by state actors that "fall short of acts of war" but seeks to "destabilise, harm and undermine" a target state; it spans "illicit financial influence", "malign political and social influence", "investment in force projection measures" and "cyber-attacks". RUSI (n.d.) notes that such activity can range "from corruption to coercion to manipulation" and the "opportunistic exploitation" of protective gaps, aiming to "disrupt democratic processes, destabilise regions and compromise critical infrastructure", and is "often hard to detect, attribute and counter". Non-state actors such as organised criminal groups or terrorist organisations may also contribute to, enable or be interwoven with state threats, including in ways that serve overlapping objectives (Kiepe 2021). Where the evidence demonstrates such connections, the review will flag them. While some governments use the term "state threats" with a similar definition to RUSI's (see M15 2026; US Department of State 2026), it is far from a universally endorsed term; indeed, "nation-state threats", "state-linked threats" or "hybrid threats" are all alternatives variously employed by actors in security circles.

This paper focuses on a subset of state threats that are most consistently identified in the literature as intersecting with financial secrecy. In particular, it examines access to strategic sectors, cyberthreats, strategic corruption and political interference. While best not understood as a threat in itself, the paper also explores the secondary tactic of sanctions evasion schemes that hinder countermeasures designed to address other state threats. These topics are selected not because they exhaust the range of national security risks posed by states but because existing research repeatedly demonstrates how opaque corporate structures, weak beneficial ownership disclosure, and other related regulatory gaps enable these forms of activity.

Access to strategic sectors

The penetration of, or access to, strategic and sensitive sectors is treated here as a state threat insofar as financial secrecy can be used to obtain leverage over areas such as media, defence, energy or dual-use production, and thereby gain leverage over critical assets, information or supply chains that may pose a national security risk (Kiepe 2021).

From a financial secrecy perspective, the evidence tends to document mechanisms that reduce the visibility of control over entities connected to strategic projects or assets, such as state actors' control over media entities in a foreign country (see case study 1). Media ownership by foreign states poses a national security risk when broadcasting and distribution is designed to unduly influence public opinion and policies (Kiepe 2021)

Case study 1: Global CAMG Media Group

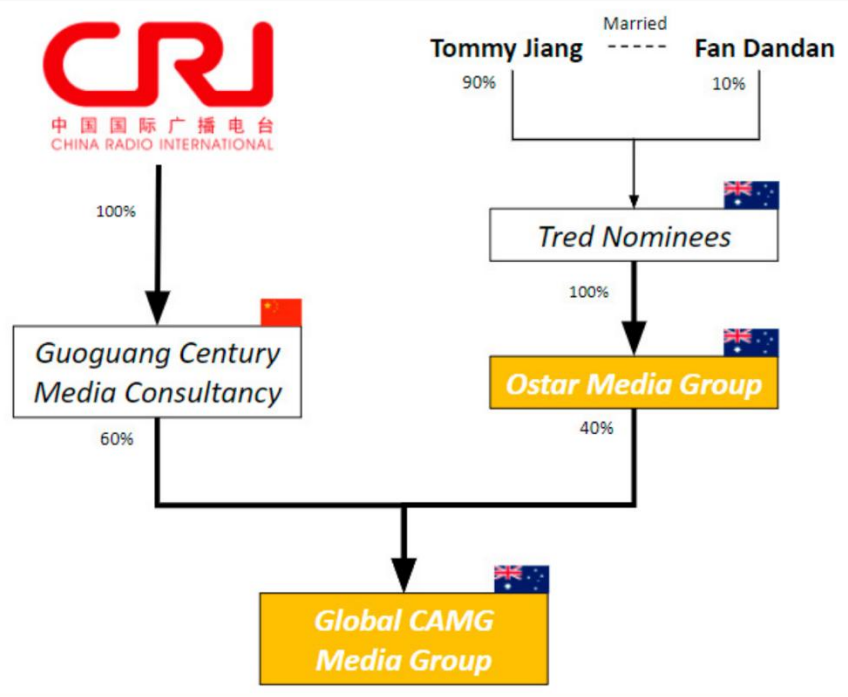
Global CAMG Media Group, headquartered in Melbourne, was part of a wider network of nominally independent radio stations that broadcast content originating from China Radio International (CRI) – a Chinese state-run international broadcaster – in Australia (Lim 2015; Lim and Bergin 2018). Global CAMG was one of three media companies that functioned as part of a covert network of 33 radio stations running CRI content in 14 countries. The firm, and local joint venture Ostar, operated at least 11 of these stations in Australia, broadcasting content aimed at Australia's Mandarin-speaking population (Lim 2015; Lim and Bergin 2018).

Lim and Bergin (2018) argue that CRI radio stations functioned as an arm of China's wider "media warfare" which seeks to influence public opinion overseas on foreign or domestic policy matters concerning China's Communist Party. Joske et al. (2020: 18) note CRI is "subordinate to the CCP Central Committee's Propaganda Department that was amalgamated with other state-owned media outlets into China Media Group".

Obscuring state-linked ownership

Global CAMG was reportedly established by a local resident in Melbourne, Tommy Jiang, and its ownership structure was reportedly deliberately designed to obscure its connection to the Chinese state (Lim and Bergin 2018). The company was 60% owned by a Beijing-based group, Guoguang Century Media Consultancy, which was itself owned by CRI through two intermediaries (Joske et al. 2020; Lim 2015; Lim and Bergin 2018).

Figure 1 : Global CAMG's ownership structure



Source: Joske et al. 2020: 56.

Global CAMG had reportedly attempted to portray itself as an independent Australian media outlet despite its close links to the Chinese state. This was achieved through front facing ownership by Australian company Ostar Media Group, and that company's ownership by Tred Nominees, which had two shareholders, Tommy Jiang (90%) and his wife Fan Dandan (10%), the former having alleged ties to the Chinese state (Joske et al. 2020).

At a 2012 National People's Congress press conference for foreign media, Chinese officials repeatedly selected favourable questions from an apparent Australian correspondent, Andrea Yu, who was later shown to be accredited to Global CAMG. Reporting indicates a similar pattern was repeated by another Global CAMG employee at an official press conference two years later (Joske et al. 2020: 57).

In response to such state threats, a number of countries have introduced or expanded foreign investment screening regimes to prevent ownership or control in strategic and sensitive sectors by foreign threat actors (European Commission 2025; Bak 2021; Kiepe 2021). The European Commission (2025) reports that by the end of 2024, 24 EU member states had foreign direct investment screening legislation in place, with many updating or expanding existing regimes. For example, Slovakia's Critical Infrastructure Act requires firms operating in designated critical sectors to notify and

obtain government approval for changes in ownership structures, while the UK's National Security and Investment Act establishes a separate screening regime for significant acquisitions and investments in sectors considered relevant to national security (Bak 2021: 21). In this sense, evidence highlights an increasing concern over threat actors exploiting vulnerabilities for strategic investment purposes (see Chupilkin et al. 2023; European Commission 2025).

Regulations and international standards also extend to media ownership as a means to prevent undue influence over public opinion by state-threat actors. The 2024 OECD recommendation on lobbying and influence (OECD 2024) calls for requiring "disclosure of conflict-of-interest situation between the media content and the private interests of the owner(s), as well as transparency around all sponsored content and advertising" and encouraging "media companies to establish integrity standards on …[sic] dealing with external pressure from lobbying and influence actors aiming to influence coverage…and interacting with partners or funders". A national example comes from Ukraine's 2021 "anti-oligarch" law, which introduced a register targeting individuals with significant media influence linked to corruption (Kiepe 2021).

Kiepe (2021) notes public procurement fraud and corruption, especially in sensitive sectors, as another pathway through which the exploitation of financial secrecy can create national security risks. This is relevant because governments frequently impose ownership related eligibility criteria on suppliers in public procurement, particularly in sensitive sectors such as defence and security (Kiepe 2021). While this strand of evidence is not always framed as explicit state threat activity, Kiepe (2021) emphasises that "[procurement] fraud and corruption as a threat to national security can be committed by both non-state actors and state actors, including corporations with links to states".

Here, shell companies are used to enter restricted or non-advertised tenders and to win contracts that were intended for vetted suppliers, which Kiepe (2021) argues poses a significant national security threat. In some cases, such activity can result in sensitive contracts being awarded to ineligible firms, the supply of defective or non-conforming parts, and the sharing of sensitive military technical material and blueprints to foreign actors (see case study 2). Case evidence also found that shell networks and anonymous ownership records were used to conceal the origin of prohibited equipment in procurement supply chains (Kiepe 2021). Kiepe (2021) therefore notes beneficial ownership transparency as crucial to helping governments identify with whom they entrust the supply of critical goods, services and sensitive information.

Case study 2: Allied Components LLC and procurement fraud

The US Department of Defense (DoD) awarded a contract to a New Jersey firm, Allied Components LLC, to supply "wing pins" for F-15 fighter jets (Voreacos and Weinberg 2020). The reporting indicates Allied Components functioned as a shell contractor that concealed an overseas manufacturing partner in India without disclosing this to the DoD.

US authorities stated that technical drawings were transferred to the unknown manufacturer without the required approvals under export controls, and that the manufactured parts were found to be defective (Voreacos and Weinberg 2020). The winning bidder later pleaded guilty to making a false claim on the contract and to an Arms Export Control Act violation tied to transmitting sensitive military technical data to India. In this context, the reporting emphasised that "in the absence of… transparency, the Defense Department [faced] financial and national security risks in its supply chain".

Shell company contracting to obscure the true supplier

As Kiepe (2021) notes, shell companies can create acute due diligence and verification gaps for public buyers in sensitive sectors, posing significant national security risks. This case shows the mechanism in practice: a US registered shell contractor served as the visible counterparty for a defence contract, while the real production chain sat with an undisclosed manufacturer in India (Voreacos and Weinberg 2020). The shell contractor obscured the manufacturing relationship by keeping the Indian corporation out of the information provided to the DoD, thereby misrepresenting where and by whom the parts were produced. That opacity reduced the buyer's ability to verify who was actually making the component and where, and it enabled sensitive military drawings to be shared with a foreign actor.

The US Government Accountability Office has reported that ownership information for approximately one-third of high-security buildings leased by the US government were unavailable (Vittori 2017). This arguably has serious national security ramifications because it limits authorities' ability to assess whether government facilities are being rented to hostile foreign states or criminal networks.

The effect of accessible and public beneficial ownership data has been tested by Collin et al. (2025), who found that the introduction of a public beneficial ownership register for overseas entities in the UK resulted in a significant and persistent decline in new property purchases via tax-haven companies, especially linked to Russian actors. This, they state, shows "that those wishing to anonymously invest in UK property viewed the policy as a threat" (Collin et al. 2025: 34) and highlights how the

existence of a beneficial ownership register with accessible information deters anonymous and potentially illicit investment into UK real estate.

Cryptocurrencies represent another area in which the use of financial secrecy intersects with state threats, including the financing of sabotage linked to Russia, which, according to Redlowska et al. (2026), may constitute activities detrimental to strategic sectors such as damaging undersea cables. These activities may be enabled by the pseudonymous nature of many crypto transactions and the availability of informal over-the-counter (OTC) crypto services that allow conversion into cash with minimal or no customer identification or regulatory oversight and no requirement for the verification of the source of funds (Redlowska et al. 2026). Investigative reporting has found that OTC services provide a route for Russian operatives to be paid in Ukraine and elsewhere, with one cash desk controlling crypto addresses that have processed millions of dollars in transactions, including assets linked to sanctioned Russian crypto services allegedly used to finance spies and informants globally (Woodman 2025).

Cyberthreats

Cyberthreats are treated here as a state threat insofar as financial secrecy can be used to resource, conceal and monetise hostile cyber activity by state actors and state-aligned networks (Bak 2021; Bernhard et al. 2024; NCSC 2025). The outcomes of these activities are increasingly recognised as posing among the most significant national security risks faced by states (NCSC 2025). State-linked actors can abuse financial secrecy to reduce the attribution of cyber threats, sustain operations or give such operations a legitimate looking commercial cover (see case study 3).

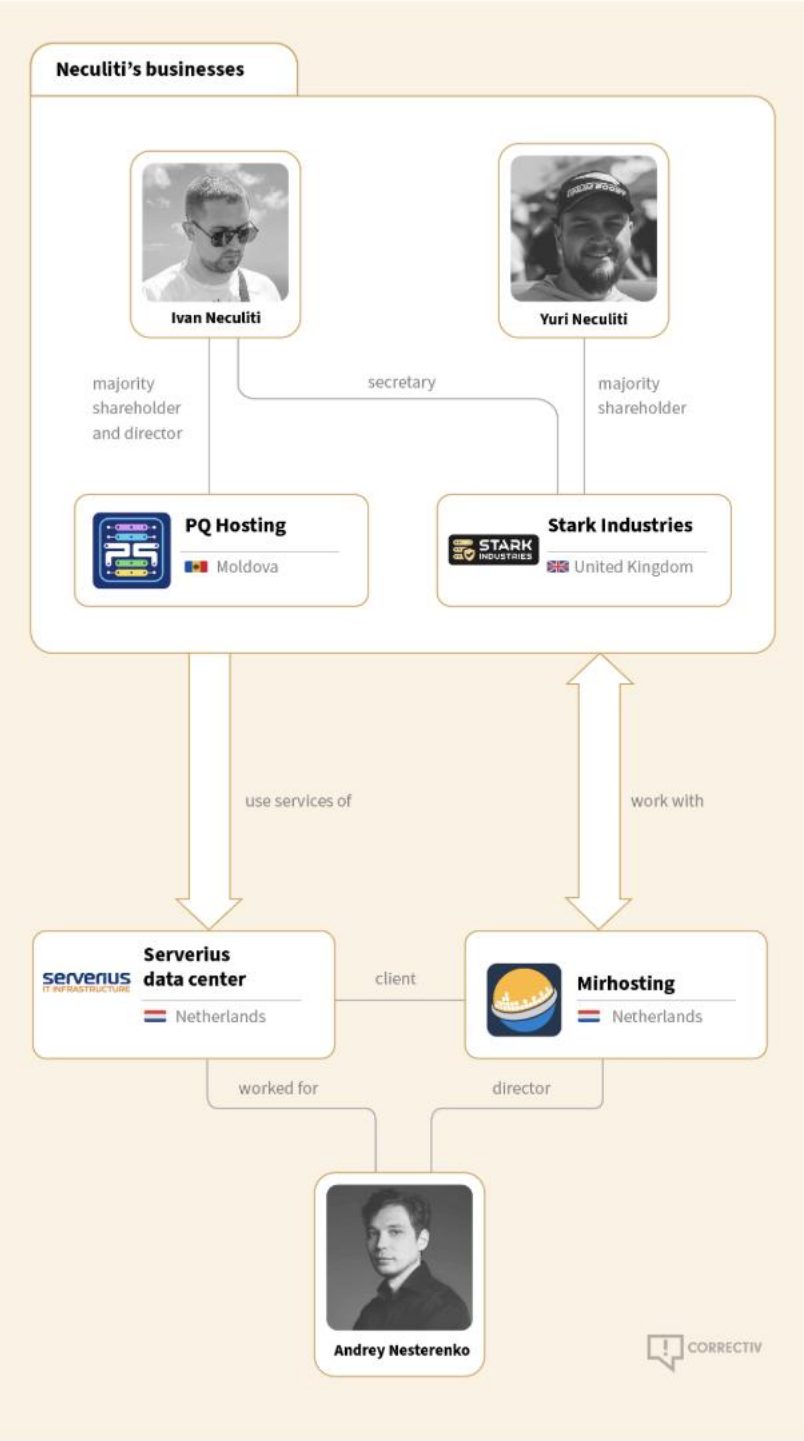
Case study 3: shell company hosting network supporting Russian aligned cyberthreats

Since Russia's full-scale invasion of Ukraine, disruptive attacks and propaganda distribution have repeatedly targeted European public services and information environments (Bernhard et al. 2024). An investigation by CORRECTIV traced hosting infrastructure linked to two Moldovan brothers and uncovered connections to both a Russian aligned influence outlet, Recent Reliable News, and DDoS activity attributed to the NoName057(16) hacktivist network, with servers operating from within an EU data centre environment in the Netherlands (Bernhard et al. 2024). The same infrastructure is linked in the reporting to alleged use by Kremlin linked actors in attacks directly targeting Ukraine (Bernhard, et al 2024).

Obscuring the service provider through a UK shell company

CORRECTIV report that the hosting service was routed through a UK registered shell company (Stark Industries Solutions) that sat between the underlying host (PQ Hosting) and wider infrastructure (Bernhard et al. 2024). PQ Hosting ran the servers in a Dutch data centre near Amsterdam, but the UK shell company was the name placed on the hosting as the outward-facing provider. So, when that infrastructure was traced, it showed up under the UK company's name first, not PQ Hosting. This arrangement masked PQ Hosting as the underlying provider and created a buffer between the activity running on the servers and the host actually supplying them, so the cyberthreat activity was not immediately traceable to the original operator (Bernhard et al. 2024).

Figure 2 : PQ Hosting's infrastructure



Source: Bernhard et al. 2024.

Andrey Nesterenko, an employee of the Netherland's based data centres, was previously connected to separate pro-Russian cyber-attacks against Georgia and his current firm, where he is director, has also reportedly been used in pro-Russian hacking activities in recent years (Bernhard et al. 2024).

Another relevant illustration is the repeated documentation that North Korean state-sponsored cyber activity is used to generate revenue for prohibited state programmes, such as nuclear and ballistic missile activities (UNSC 2024). Bak (2021) highlights that these North Korean networks often rely on chains of anonymous shell companies made up of ever-changing front men that move addresses and change identities. By the time compliance professionals have completed due diligence and know-your-counterpart checks or investigators uncover a scheme, the ownership structure has often already shifted or a new front person has taken over (Rosenberg and Bhatiya 2020).

Foreign political interference

Foreign political interference may generate national security risks where financial secrecy enables such activity to shape political processes, constrain policy choices or influence decision-makers in ways that are opaque to regulators and voters (Bak 2021; Rudolph and Morley 2020; Kiepe 2021; Valldares and Sample 2022).

One of the most prominent forms of interference is covert forms of political finance. Rudolph and Morley (2020) identified 115 cases in the 2010s where governments directed an estimated US$300 million into covert interference in democratic or political processes across over 30 democracies, with the frequency of attacks growing exponentially since 2014. This tool of foreign interference involves state-linked actors channelling funds to foreign political parties, candidates, campaigns, well-connected elites or politically influential groups. However, these concerns are not limited to overtly illegal activity or proven electoral manipulation, and can involve the use of traditional financial channels such as loans or donations (Alliance for Securing Democracy and C4ADS 2018), lobbying (Harding et al. 2017a; 2017b; Sullivan and Radu 2017).

Over the last two years international commitments have placed emphasis on restrictions to foreign state influence actors. In 2024, the OECD made several recommendations to ensure transparency of lobbying includes such actors (OECD 2024). Further, the Conference of the States Parties to the United Nations Convention against Corruption (UNCAC CoSP) called for governments to place restrictions or prohibitions on donations by foreign owned or controlled legal entities, as well as for taking measures against using the funding of foreign political parties in trading in influence and foreign bribery. Against this backdrop, many countries have begun to place heavy regulatory constraints on foreign funding of their political processes, such as bans on donations by non-nationals (see International Idea n.d.a) or funding and disclosure requirements (see International Idea n.d.b). In particular, gaps in financial transparency can weaken these safeguards by obscuring the true source of political funding.

From a financial secrecy perspective, evidence connecting state-linked covert foreign political finance to illicit finance tends to document mechanisms that reduce the visibility of politically relevant financial relationships or funds. One key mechanism involves the use of corporate entities with opaque ownership or control to create a channel for state-linked interests to operate inside a democratic framework without any clear attribution (see case study 4) or to allow control over funds to be shifted between entities, preserving political-financial relationships linked to foreign states (see case study 5).

Where beneficial ownership is weakly enforced or where information is inaccessible or unreliable, state-linked corporate vehicles can be used to channel politically motivated funds from states to influence foreign democratic or political processes (see FATF and Egmont Group 2018).

Case study 4: the case of Gazprom and covert foreign political finance

Gazprom, a Russian state-controlled corporation, is the largest producer of natural gas in the country, the only owner of the nationwide gas transmission system and the sole exporter of piped gas out of Russia (Krutikhin 2021). Krutikhin (2021: 189), describes Gazprom as an "instrument of strengthening and expanding Russia's footprint in the economies of European nations" (Krutikhin 2021: 189).

Gaps in Germany's beneficial ownership verification

In February 2022, Transparency International (2022b) reported that a German state-owned climate and environmental protection foundation was funded with more than US$300,000 of taxpayer money and a further US$24 million from the pipeline project Nord Stream 2, which was owned by Gazprom International Projects LLC, a subsidiary of Gazprom. Reuters reported that the regional premier of Mecklenburg-Vorpommern backed Nord Stream 2 publicly and initiated legislation to set up the foundation, with a charter that enabled support for completing the pipeline (Escritt and Marsh 2022).

Nord Stream 2 was authorised to propose the managing director for the foundation's business division, have control over its funds and assets, and to assign board members. Reporting also indicates that, while the stated goal of the foundation is climate and environmental protection, it actively supported the construction of the pipeline (Solomon 2021; Transparency International 2022b). Reuters also reported on links between the pipeline, SPD leadership figures in the state, and Moscow, including the role of former Chancellor Gerhard Schroeder, who subsequently held senior positions at the company behind Nord Stream 2 (Escritt and Marsh 2022).

Transparency International (2022b) noted that the foundation's entry in Germany's corporate register omitted its tie to Gazprom due to the absence of a beneficial ownership verification mechanism. This created a vehicle through which Russian state-linked commercial interests could exercise influence within a European legal and political framework without any formal legal association.

Bressanelli (2021) described an alleged planned scheme connecting the Russian state to a complex network of intermediaries and shell companies to covertly channel funds into the Lega party in Italy (Bressanelli 2021). The alleged process involved a

Russian state-linked oil company selling at least 3 million metric tons of fuel over a year to an Italian oil company, Eni, for approximately US$1.5 billion. The Italian company would receive the oil at a discounted rate, generating a profit of US$65 million, funds which would then be covertly channelled to the Lega party via intermediaries (Horowitz 2019). However, it was unclear whether the deal ever went ahead, and the party and associated companies deny ever having received funds or any involvement in the alleged scheme (Bressanelli 2021).

Case study 5: First Czech Russian Bank loan to France's National Front

A case of foreign political financing

In 2014, the First Czech Russian Bank (FCRB), a Russian-domiciled bank, issued a €9.4 million loan to France's National Front, a far-right political party. The loan was lawful under French campaign finance laws, which permit loans from foreign entities (Alliance for Securing Democracy and C4ADS 2018).

At the time the loan was issued, FCRB was already implicated in a range of high-risk financial activities. Reporting later showed that the bank had facilitated trade with Iranian clients while Iran was under international sanctions, held funds linked to the Central Bank of Iran, and played a role in large-scale illicit financial flows through the Russian Laundromat[2] (Alliance for Securing Democracy and C4ADS 2018). According to Alliance for Securing Democracy and C4ADS (2018: 1), the evidence demonstrates a case of "Russian state-sanctioned interference in the Western political system".

Maintaining politically sensitive financial relationships via private entities

In early 2016, FCRB approached insolvency, and a subsequent litigation process concerning alleged self-enrichment by senior management led to court proceedings and asset disclosures that exposed the bank's client base and lending practices. It revealed an opaque, ad-hoc network of senior Russian government officials who had helped to arrange the National Front loan through the private bank, which created a layer of deniability (Alliance for Securing Democracy and C4ADS 2018). When FCRB entered bankruptcy proceedings in 2016, this network did not abandon the loan. Instead, the loan was briefly moved to a shell company with limited commercial activity, before being reassigned to Aviazapchast JSC, a private aviation company

[2] "FCRB was one of 19 Russian financial institutions implicated in a $20 billion capital flight and laundering scheme that moved money out of Russia into European accounts through Moldova and Latvia between 2011 and 2014" (Alliance for Securing Democracy and C4ADS, 2018: 5)

closely involved in strategically significant partnerships for the Russian state, including defence exports (Alliance for Securing Democracy and C4ADS 2018).

While the motivation for the transfers and the continuing political interest in the loan remained unclear, the reassignment of the loan claim between closely connected private entities ensured that the politically sensitive financial relationship with the National Front persisted, even as FCRB – a node tied to state-linked and illicit financial networks – entered insolvency proceedings and legal scrutiny.

RUSI notes that state-threat actors increasingly view virtual assets such as cryptocurrencies as "as an important tool of statecraft" (Barnett 2025). From this perspective, virtual assets expand the range of methods available for obscuring funds, including influencing democratic or political processes.

State-linked actors may use cryptocurrency to route funds through jurisdictions with limited regulation, allowing those funds to be converted and ultimately used for political donations. Additionally, crypto "mixers" may allow state-linked actors to disguise the origin of funds and channel ostensibly "clean" cryptocurrency or funds to political donors (Spotlight on Corruption 2025).

Moldovan authorities and international investigators have documented the distribution of millions of dollars of funds via a Russian linked stable coin, A7A5, and its associated networks to influence electoral outcomes, support anti-government protests and facilitate vote buying in referendums in Moldova (CRI 2025; Makogon 2026). Reporting indicates that ruble-denominated funds are converted into A7A5, via a crypto exchange operating in Kyrgyzstan, a jurisdiction with gaps in regulatory oversight.

It should be noted, however, that the evidence base in this area relies heavily on public reporting and likely captures only a fraction of the underlying activity (Bak 2021). Moreover, while the pathways through which financial opacity facilitates politically sensitive funding are well documented, evidence of political outcomes – such as changes in policy decisions or election results – remains less attributable.

Strategic corruption

Traditional understandings of corruption are most often associated with financial benefits such as bribery or embezzlement. Increasingly, however, governments, researchers and anti-corruption practitioners are examining how corruption can also function as a tool for political, economic and or security gains, including the projection or consolidation of geopolitical power, largely known under the umbrella concept, "strategic corruption" (Kassa and Guy 2025).

While strategic corruption is a contested term (see Pozsgai-Alvarez and Lang 2025) for the purposes of this paper it is understood as "a state agent's use of financial or other means to incentivise a public power-holder in another country or international organisation to abuse their entrusted power for the strategic gain of the corrupting state" (Lang 2024). According to Kassa and Guy (2025), this can range from single incidents such as bribery to compromise individuals or weaken institutions in targeted jurisdictions to a strategic and long-term approach in which corrupt acts build upon each other to gradually consolidate power or pursue geopolitical objectives. This in turn may generate national security risks for target locations because democratic processes and security relevant institutions are infringed upon by foreign state-actors in the pursuit of their geopolitical goals (Baez Camargo and Kassa 2024).

While strategic corruption is frequently linked to financial secrecy (see Kassa and Guy 2025), the underlying mechanisms – particularly those relating to corporate transparency – are rarely documented in a direct or systematic way. One identified mechanism, however, involves routing funds through opaque corporate vehicles and cross-border accounts with weak anti-money laundering regulations in attempts to corrupt foreign beneficiaries in positions of political power or influence (see case study 6).

Case study 6: the Azerbaijani Laundromat

The Azerbaijani Laundromat refers to a large-scale financial network uncovered through investigative reporting, through which approximately US$2.9 billion was routed from Azerbaijan into the European financial system between 2012 and 2014, including to allegedly bribe European politicians (Harding et al. 2017a; 2017b; OCCRP 2017). Reporting shows that almost half of the funds came from a shell company linked to Azerbaijan's ruling family via a state-owned bank, with the next two largest funding channels traced to offshore companies connected to "a regime insider" (OCCRP 2017).

Further funding came directly from Azerbaijani government ministries, including defence and state security institutions, as well as from a Russian state-owned arms exporter (Crijns 2019).

While not all of the funds were politically motivated, reporting indicates that the network was used in part to channel funds toward lobbying and other forms of political engagement abroad. For example, payments to former Parliamentary Assembly of the Council of Europe (PACE) member Luca Volontè were reportedly discovered by Italian authorities, funds that prosecutors allege were paid to mute criticism of Azerbaijan's human rights record within the assembly (Ismayilova 2017).[3] Additionally, leaked bank records reveal multiple payments to several other former members of the Council of Europe's parliamentary assembly, representing efforts to corrupt officials (Harding et al. 2017b). In 2026, a German court handed down a suspended prison sentence to a former German MP for accepting payments from Azerbaijani officials in return for voting and making statements in favour of Azerbaijan during PACE sessions, as well as sharing confidential documents (Dowsett 2026).

Using shell companies to obscure the movement of funds

Reporting shows that funds entered the European financial system via four UK registered companies whose beneficial owners were not publicly known (Harding et al. 2017a; OCCRP 2017) and highlights that the companies were structured in such a way to be "purposefully opaque" (Harding et al. 2017b). While the UK has a beneficial ownership register, at the time, there was no requirement for verification of the registered data, and any owner or manager of any company could easily register false information (Transparency International 2017).[4] For the case, this meant no reliable link could be established between the companies channelling the funds and the state-linked actors associated with their source.

The companies also had bank accounts in Estonia, where anti-money laundering checks were inadequate at the time (Harding et al. 2017a). This meant the transferred funds were processed within the European Union without effective scrutiny of their origin or purpose (Transparency International 2017). Many other payments were transferred across other secret shell company networks similarly registered in the UK, indicating that the full extent of the scheme is largely unknown (OCCRP 2017).

[3] While Volontè was sentenced to four years' imprisonment in 2021, this was overturned, and he was acquitted by an appeal court the following year (Ferrarella 2022).

[4] Recent reforms in the UK, through the Economic Crime and Corporate Transparency Act 2023, seek to close these loopholes. It requires all directors, people with significant control and those who file with Companies House to verify their identity using government issued identification (Companies House 2025).

Transparency International (2017) notes that several features made the UK particularly attractive for misuse at the time, including the low cost of incorporation, the speed and simplicity of company formation, and the UK's respectable business reputation, which lent legitimacy to shell companies.

The use of sanctions evasion to facilitate state threats

It is widely understood that sanctions evasion is in itself an illicit finance activity (Lewis and Prelec 2022: 6). Countries may impose sanctions against individuals,[5] economic sectors or whole economies as a countermeasure in response to geopolitical actions or in response to state threats (HM Government 2023: 47). Sanctions evasion, while not inherently representing a state threat itself, can thereby undermine such countermeasures and is used to diminish their retaliatory and deterrence effects. In addition, this paper recognises that sanctions evasion represents a necessary "tool" used by state actors to facilitate continued state threats (such as those outlined in this paper) in the face of retaliatory sanctions.

Sanctions issued in response to state or national security threats often aim to curtail proliferation and military financing. While such activities are typically addressed within security narratives as forms of money laundering, terrorist financing or illicit transfer of funds (see FATF 2025; HMRC 2023), they are considered here in terms of how financial secrecy for sanctions evasion enables or sustains activity linked to state threats, such as the financing of prohibited weapons programmes, dual-use procurement networks, or military operations and capabilities (FATF 2025) as well as financing sabotage.

The main types of sanctions relevant to financial secrecy are economic and financial sanctions, such as restrictions on trade and financial transactions. In practice, sanctions against states often respond to national security threats, focusing on state-owned entities or security relevant sectors such as military, energy or technology (see Kiepe 2021; Mallory 2021), as well as high-ranking officials. Individual sanctions often entail asset freezes and travel bans (see Nice 2022).

Evidence on sanctions evasion linked to proliferation and military financing documents the intersection with corporate and financial secrecy through the use of shell and front companies, layered transactions and third-country access to mask relationships to state-linked actors and obscure the destination or use of certain goods (FATF 2025; Kharon 2022; LSEG 2025). FATF (2025) also notes the role of professional enablers, such as lawyers and accountants, who establish complex

[5] Individual sanctions may be designated to counter such threats but also other issues such as human rights violations and corruption, notably the so-called Global Magnitsky sanction regimes.

structures, as well as freight forwarders or shipping agents, who create opaque supply chains.

The literature identified the Democratic People's Republic of Korea (hereafter North Korea) as one of the most prolific actors when it comes to using financial secrecy to evade sanctions imposed in response to investment into nuclear and ballistic missile capability. Mallory (2021) documented evidence from 15 reports produced between 2010 and 2021 by the United Nations Security Council Panel of Experts (UNSC POE) that monitors UN sanctions imposed on North Korea as case evidence of North Korean sanctions evasion networks. The review highlighted that North Korea uses financial secrecy to facilitate sanctions evasions for proliferation financing in the following ways (Mallory 2021):

- register front and shell companies using false information, employing North Koreans under non-official cover
- using foreign agents (and "trusted partners") to register front companies, open accounts and transact on behalf of North Korean networks
- using local front company structures (e.g., a "representative office") to obtain hard-currency bank accounts and access to the international financial system
- holding and moving value through accounts of front companies, shell companies and trusted partners, including returning hard currency outside the banking system

Mallory (2021) also notes that North Korea frequently exploits financial secrecy in countries where anti-money laundering and countering the financing of terrorism rules are poorly enforced. They argue that poor enforcement can be attributed to a variety of causes, including low domestic capacities, officials' lack of understanding of sanctions or the need for them, or the absence of political will.

Case study 7: Daedong Credit Bank's (DCB) ledger based network for North Korean overseas payments

This case study describes a North Korea government–controlled system used to move payments internationally and is substantiated by evidence documented by UNSC POE (Mallory 2021: 36). As reflected throughout Mallory's (2021) analysis, North Korea's covert financing mechanisms limit the observability of transaction-level end use, but can nonetheless be linked to proliferation related financing.

A centrally maintained ledger, managed by DCB, was used to track debits and credits across multiple overseas entities, enabling designated North Korean firms to pay foreign suppliers and receive customer payments abroad. When balances needed to

be replenished or surpluses extracted, the network relied on occasional top-ups, withdrawals and the physical movement of cash.

Obscuring sanctioned counterparties via front companies

The mechanism centred on routing transactions through North Korean–controlled front companies that were not registered as financial entities in their host countries. When a sanctioned firm needed to pay a foreign supplier, a joint venture or overseas representative would initiate transfers from accounts they controlled, often via an additional front company in a third jurisdiction. Customer payments for North Korean services were similarly directed into overseas front company or representative accounts that did not appear on the original trade paperwork, weakening the traceable link between commercial activity and financial flows.

Deniability, reduced bank visibility and harder tracing

Structuring payments this way reduces the chance that compliance screening will identify a designated North Korean entity because the visible payer and immediate transaction chain is made to appear as though it is not from a North Korean entity. By keeping the process within a central ledger, the network minimises the number of cross-border transfers that might trigger sanctions screening, relying instead on front company opacity to prevent attribution to a designated North Korean entity; this occurs when financial institutions' obligations to identify and verify beneficial owners are not implemented appropriately. The overall effect is to sustain procurement and revenue generation under sanctions by creating layers of separation from the true beneficiary/origin.

A 2025 US enforcement action provides another illustration of a shell company function in connection to North Korean sanctions evasion (US Department of Justice 2025). In summarising court filings, the US Department of Justice describes US based facilitators creating shell companies with matching websites and financial accounts to make overseas North Korean remote IT workers appear affiliated with legitimate US businesses. Those shell entities then served as the "front" through which US companies paid for the work, with funds subsequently moved overseas (US Department of Justice 2025).

Similar corporate transparency vulnerabilities are also exploited by other sanctioned states. Some schemes rely on embedding front companies within reputable jurisdictions and using private control arrangements, such as "trustee agreements" and nominee directors, to obscure ownership and traceability (see case study 8).

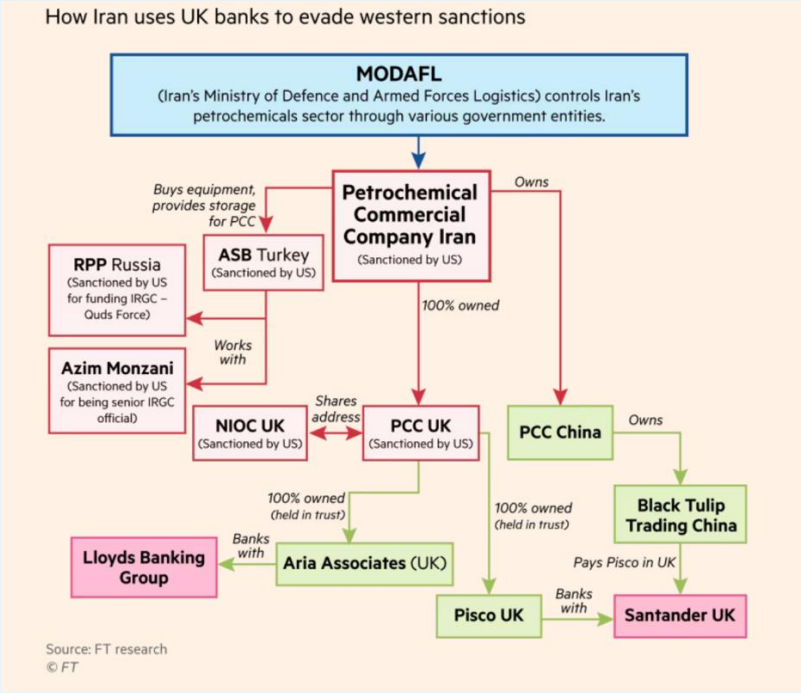
Case study 8: exploiting UK bank accounts for Iranian sanctions evasion

Reporting by the Financial Times revealed that two of the UK's biggest banks – Lloyds and Santander UK – provided accounts to front companies with connections to a sanctioned Iranian petrochemicals company (PCC) (Johnson et al. 2024). The state-linked firm, PCC (see US Department of the Treasury 2022) and its British subsidiary PCC UK, have been under US sanctions since November 2018 and have been described by US authorities as being connected to networks involving Iran's Islamic Revolutionary Guard Corps' foreign operations units and Russian intelligence agencies to raise money for Iranian proxy militias (Johnson et al. 2024).

Obscuring ownership through nominee arrangements

PCC used front companies in the UK to receive money from Iranian proxy entities operating in China while hiding the true beneficial owners through "trustee agreements" and the use of nominee directors.

Figure 3: How Iran's petrochemicals sector uses UK banks to evade western sanctions



Source: Johnson et al. 2024.

Some corporate networks used to obscure ownership and control over assets use nominee arrangements as they allow an individual to appear, on paper, as a legal owner, while control and decision-making remains with an undisclosed party (Trider n.d.). For example, according to the UK corporate registry, Pisco UK (see Figure 3) was fully owned by a British national, while leaked internal documents revealed the firm was fully controlled by PCC. The British national acted as a nominee by having signed an agreement to own the company in trust on PCC's behalf (Johnson et al. 2024), although the British national was still listed as the BO of the company, possibly in violation of UK regulations.[6]

The expected effect is that payments can be directed into a "safe" UK account and processed under the name of a "permissible" legal owner, while financial connections to the ultimate owner (in this case PCC) are hidden.

Empirically, research suggests that sanctions can also reshape where and how assets are held across jurisdictions, including those that provide for corporate and financial secrecy. Using the Bank for International Settlements cross-border deposit data alongside US and EU sanctions data (1996–2015), Langenmayr, Tovmasyan and Vosseler (2025) find that financial sanctions targeting threat actors are associated with increases in deposits in offshore financial centres. They corroborate this pattern with a synthetic control case study of Russia following the 2014 annexation of Crimea, estimating an approximately 15% post-sanctions increase in Russian deposits in tax havens (Langenmayr, Tovmasyan and Vosseler 2025).

While this evidence extends beyond proliferation and military financing sanctions, it suggests that sanctions imposed after major geopolitical events can be followed by measurable shifts in financial secrecy patterns, which may represent attempts to undermine the effectiveness of such sanctions.

The literature also highlights some measurable corporate transparency impacts following the Russian invasion of Ukraine in 2022. Allison et al. (2023) documents some country case evidence[7]:

- Turkey: research shows that incorporations of foreign-owned companies increased by 50% in 2022 compared with 2021
- Kazakhstan: approximately 4,000 new Russian owned companies were registered in the first nine months of 2022, compared to a stock of 11,000 before 2022,

[6] For more information on nominee ownership arrangements, including how arrangements are structured with unknown nominators, see Open Ownership (n.d.).

[7] While these trends indicate significant shifts in corporate activity following the Russian invasion of Ukraine, they should not be interpreted as evidence of sanctions evasion in themselves as businesses may be legitimate enterprises established by individuals relocating from Russia.

suggesting that nearly a quarter of all Russian owned companies in the country were established at the start of 2022

- Georgia: more than 6,400 new Russian owned companies were registered between March and July 2022, seven times the number recorded over the same period in 2021
- United Arab Emirates: in the first month after the full-scale invasion, Russian citizens registered approximately 500 companies

Investigative reporting also documents the use of overseas real estate as an asset holding and concealment mechanism for sanctions evasion. For example, reporting by OCCRP (2020) shows that relatives of sanctioned Venezuelan defence minister Vladimir Padrino López controlled at least 14 properties in the US alongside a network of corporate entities. These assets were held through family members and corporate vehicles rather than in the sanctioned individual's name, allowing continued access to the US property market and financial system despite sanctions (OCCRP 2020). Sanctions evasion by senior defence figures signals impunity and undermines the effectiveness of sanctions regimes designed to contain and deter security violations.

More broadly, FATF (2025) highlights that exposure to vulnerabilities related to proliferation financing are often shaped by a country's geographic position within trade, transport and financial networks. Many jurisdictions report a heightened risk where they function as international financial centres, namely due to the breadth of products and services that can be repurposed by illicit procurement networks (FATF 2025: 16–20). Vulnerabilities also arise from ongoing economic and trade relations with sanctioned jurisdictions as well as from geopolitical alignments, dependencies or historical links, which can create opportunities for threat actors to access financial systems or channel funds without the host jurisdiction's awareness (FATF 2025). While such factors do not always concern financial secrecy, FATF (2025: 18) notes that vulnerabilities deepen where beneficial ownership transparency frameworks are weak:

> 'Difficulty accessing [beneficial ownership] information impedes cross-border investigations by authorities seeking to identify and trace the [proliferation financing] path, especially when multiple countries with inconsistent legal frameworks are involved.'

Therefore, access to reliable beneficial ownership data enables authorities to detect ownership and examine links across front and shell companies and to support cross-agency due diligence on sanctioned asset types, helping to identify and disrupt sanctions evasion networks (Kiepe 2021).

References

Alliance for Securing Democracy and C4ADS. 2018. Illicit Influence – Part One – A Case Study of the First Czech Russian Bank. German Marshall Fund.

Allison, O., Hack, A.A., O'Shea, L. and Saiz, G. 2023. Illuminating the Role of Third-Country Jurisdictions in Sanctions Evasion and Avoidance (SEA). SOC ACE Research Paper No. 21. Birmingham: University of Birmingham.

Azmi, M.N.B.L. 2025. Espionage and Securitization. in: the Age of Global Conflict: Intelligence, Perception, and Peacebuilding. Security Science Journal, 6(2), Pp.118-137.

Baez Camargo, C. and Kassa, S. 2024. How (Strategic) Corruption Fuels Insecurity by Affecting Power. Basel Institute on Governance.

Bak, M. 2021. Illicit Finance and National Security. U4 Anti-Corruption Helpdesk Answer.

Barnett, N. 2025. UK Election Security is Threatened by Political Money Laundering via Cryptocurrency.

Baysal, B. 2020. 20 Years of Securitization: Strengths, Limitations and a New Dual Framework, Uluslararasi Iliskiler, Vol. 17, No. 67, 2020, Pp. 3-20.

Bernhard, M., Hock, A. and Thust, S. 2024. Hacks and Propaganda: Meet the Two Brothers Bringing Russia's Cyber War to Europe. Correctiv.

Berzina, K. and Soula, E. 2020. Conceptualizing Foreign Interference in Europe.

Bressanelli, E. 2021. Investing in Destabilisation: How Foreign Money is Used to Undermine Democracy in the EU.

Brimbeuf, S., Martini, M., Hollenbach, F. and Szakonyi, D. 2023. Behind a Wall: Investigating Company and Real Estate Ownership in France. Transparency International France and Anti-Corruption Data Collective.

Centre for Information Resilience (CRI). 2025. A7A5: Circumventing Sanctions with Stablecoin Cryptocurrency.

Chupilkin, M., Javorcik, B. and Plekhanov, A. 2023. The Eurasian Roundabout: Trade Flows into Russia through the Caucasus and Central Asia.

Collin, M., Hollenbach, F.M. and Szakonyi, D. 2025. The End of Londongrad? Ownership Transparency and Offshore Investment in Real Estate.

Companies House. 2025. Verifying Your Identity for Companies House.

Conference of the States Parties to the United Nations Convention against Corruption (UNCAC Cosp). 2025. Resolution 11/7: Preventing and Combating Corruption through Enhancing Transparency in the Funding of Political Parties, Candidatures for Elected Public Office, and Electoral Campaigns.

Crijns, D. 2019. The Azerbaijani Laundromat: a New Money Laundering Machine in a Familiar Guise. Anti-Money Laundering Council.

Deutschlandfunk. 2022. Schwesig, Klimastiftung und Nord Stream 2: Warum die umstrittene Stiftung in der Kritik steht.

Dowsett, J. 2026. Former German MP Gets Suspended Sentence for Azerbaijani Bribes.

Escritt, T. and Marsh, S. 2022. How a German State Helped Moscow Push a Pipeline, Weakening Ukraine. Reuters.

European Commission. 2025. Report from the Commission to the European Parliament and the Council: Fifth Annual Report on the Screening of Foreign Direct Investments into the Union (COM(2025) 632 final). Brussels, 14 October 2025.

FATF. 2025. Complex Proliferation Financing and Sanctions Evasion Schemes, FATF.

FATF and Egmont Group. 2018. Concealment of Beneficial Ownership. FATF.

Ferrarella, L. 2022. Luca Volontè e i soldi dell'Azerbaijan al Consiglio Ue: prescritta la condanna per corruzione internazionale.

Garcia-Bernardo, J., Fichtner, J., Takes, F.W. and Heemskerk, E.M. 2017. Uncovering Offshore Financial Centers: Conduits and Sinks in the Global Corporate Ownership Network. Scientific reports, 7(1), p.6246.

Goodrich, S. and Mollat, M. 2025. Trust Issues: Tackling the Final Frontier of Secret Property Ownership. Transparency International UK.

Government of Canada. No date. Understanding Foreign Interference.

Harding, L., Barr, C. and Nagapetyants, D. 2017a. Everything you Need to Know About the Azerbaijani Laundromat. The Guardian.

Harding, L., Barr, C. and Nagapetyants, D. 2017b. UK At Centre of Secret $3bn Azerbaijani Money Laundering and Lobbying Scheme. The Guardian.

HM Revenue and Customs (HMRC). 2023. Proliferation Financing, HMRC Internal Manuals: Economic Crime Supervision Handbook.

HM Government. 2023. Economic Crime Plan 2 2023-2026.

Home Office. 2026. UK Anti-Corruption Strategy 2025.

Home Office. 2025. A Guide to the National Security Act 2023 for Security Professionals. Guidance, 24 January.

Horowitz, J. 2019. Audio Suggests Secret Plan for Russians to Fund Party of Italy's Salvini. New York Times.

Injac, O. 2016. National Security Policy and Strategy and Cyber Security Risks.

International Monetary Fund (IMF). 2023. Fight against Illicit Financial Flows. Factsheet, 1.

International Idea. No date a. Political Finance Database: Is There a Ban on Donations from Foreign Interests to Political Parties?

International Idea. No date b. Political Finance Database: Do Political Parties Have to Report on Their Election Campaign Finances?

Ismayilova, K. 2017. Businessman Suspected in Italian Bribery Case Linked to Azerbaijan's First Family. Organized Crime and Corruption Reporting Project.

Johnson, M., Morris, S. and Fisher, L. 2024. Iran used Lloyds and Santander Accounts to Evade Sanctions. Financial Times.

Joske, A., Li, L., Pascoe, A. and Attrill, N. 2020. The Influence Environment: a Survey of Chinese-Language Media in Australia. Policy Brief, Report No. 42/2020. Canberra: Australian Strategic Policy Institute.

Kassa, S. and Guy, M. 2025. Strategic Corruption. Quick Guide Series No. 37. Basel: Basel Institute on Governance.

Kharon. 2022. A North Korean Sanctions Evasion Typology: Use of Complex Ownership Structures.

Kiepe, T. 2021. Using Beneficial Ownership Data for National Security. Open Ownership.

Krutikhin, M. 2021. Russia's Gazprom: A Case Study in Misused Interdependence. I DW Drezner, H. Farrell & AL Newman (Red.). The uses and abuses of weaponized interdependence, pp.185-202.

Langenmayr, D., Tovmasyan, M. and Vosseler, S. 2025. Bypassing Sanctions: Hide'N Seek in Tax Havens? (No. 12086). CESifo Working Paper.

Lang, B. 2024. Strategic Corruption. In Elgar Encyclopedia of Corruption and Society.

Lenz-Raymann, K. 2014. Securitization Theory: Legitimacy in Security Politics', in Securitization of Islam: a Vicious Circle – Counter-terrorism and Freedom of Religion in Central Asia. Bielefeld: Transcript Verlag, pp. 243–255.

Lewis, D. and Prelec, T. 2022. New Dynamics in Illicit Finance and Russian Foreign Policy. SOC ACE Research Paper No 17. University of Birmingham.

Lim, B.K. 2015. Special Report – Exposed: Beijing's Covert Global Radio Network. Reuters.

Lim, L. and Bergin, J. 2018. Inside China's Audacious Global Propaganda Campaign. The Guardian.

LSEG. 2025. International Sanctions Evasion: Four Tactics to Track.

Makogon, S. 2026. 'How Crypto Funds Russia's War'. Center for European Policy Analysis.

Mallory, K. 2021. North Korean Sanctions Evasion Techniques. Santa Monica, CA: RAND Corporation.

M15. 2026. Countering State Threats.

Nice, A. 2022. Ukraine Crisis: Financial and International Trade Sanctions. Institute for Government.

Nizzero, M. 2024. Illicit Finance As a National Security Threat: Balancing Security and Unintended Consequences. The RUSI Journal, 169(6), pp.64-76.

National Cyber Security Centre (NCSC). 2025. Annual Review 2025. London: National Cyber Security Centre.

OECD and IDB. 2024. Building Effective Beneficial Ownership Frameworks: A joint Global Forum and IDB Toolkit - Second edition, Global Forum on Transparency and Exchange of Information for Tax Purposes. OECD.

OECD. 2024. Recommendation of the Council on Transparency and Integrity in Lobbying and Influence.

Open Ownership. No date. Representing Nominee Arrangements (Beneficial Ownership Data Standard v0.4).

Open Ownership. 2022. Measuring the Economic Impact of Beneficial Ownership Transparency: A Landscape Study.

Organized Crime and Corruption Reporting Project (OCCRP). 2017. The Azerbaijani Laundromat.

Organized Crime and Corruption Reporting Project (OCCRP), 2020. The General and his Corporate Labyrinth. Revolution to Riches investigation.

Otukoya, T.A. 2024. The Securitization Theory. International Journal of Science and Research Archive, 11(1), pp.1747-1755.

Pozsgai-Alvarez, J. and Lang, B. 2025. Getting "Strategic Corruption" Right: Mapping Contested Meanings in a Changing Geopolitical Landscape. Public Integrity, pp.1-19.

Reed, Q. and Fontana, A. 2011. Corruption and Illicit Financial Flows: the Limits and Possibilities of Current Approaches. U4 Issue No. 2, January 2011. Bergen: Anti-Corruption Resource Centre (U4), Chr. Michelsen Institute.

Redlowska, K., Popyk, M. and Keatinge, T. 2026. Responding to Russian Sabotage Financing. Insights Paper, Royal United Services Institute.

Rosenberg, E. Bhatiya, N. 2020. Busting North Korea's Sanctions Evasion. Center for a New American Security, March 4.

Royal United Services Institute for Defence and Security Studies (RUSI). No date. State Threats.

Rudolph, J. Morley, T. 2020. Covert Foreign Money. The Alliance for Securing Democracy.

Spotlight on Corruption. 2025. How Foreign or Hostile Actors Could Hijack the Next General Election.

Solomon, E. 2021. German Green Foundation Joins Efforts to Complete Nord Stream 2. Financial Times.

Sullivan, D. and Radu, P. 2017. What is a Laundromat? OCCRP.

Transparency International. 2022a. Reforming Global Standards on Beneficial Ownership Transparency.

Transparency International. 2022b. Germany: State Government Conceals Gazprom's Connection to Its Controversial Environmental Foundation. Press release, 16 February.

Transparency International. 2017. The Spill-over Effects of Corruption in Azerbaijan.

Trider. No date. Nominee Directors and the Legal Fog Around Real Control.

United Nations Security Council. 2024. S/PV.9676 Security Council.

US Department of the Treasury. 2022. Treasury Targets International Sanctions Evasion Network Supporting Iranian Petrochemical Sales (Press Release JY0819).

US Department of the Treasury. 2024. Illicit Finance Strategy.

US Department of Justice. 2025. Justice Department Announces Coordinated Nationwide Actions to Combat North Korean Remote Access Trojans and Cyber Intrusions

US Department of State. 2025. Joint Statement on Iranian State Threat Activity in Europe and North America.

Valldares, J. and Sample, K. 2022. How OGP Members Can Counter Covert Foreign Political Finance.

Vittori, J. 2017. How Anonymous Shell Companies Finance Insurgents, Criminals, and Dictators. Council on Foreign Relations.

Voreacos, D. and Weinberg, N. 2020. Pentagon Shell Companies. Los Angeles Times.

Woodman, S. 2025. From Dubai to Toronto, inside the Crypto-to-Cash Storefronts Fueling Money Laundering's New Frontier, International Consortium of Investigative Journalists.

World Bank. 2023. "Beneficial Ownership Registers: Implementation Insights and

Emerging Frontiers.” Equitable Growth, Finance and Institutions Insight. Washington, DC: World Bank.

Disclaimer

All views in this text are the author(s)', and may differ from the U4 partner agencies' policies.

Corruption erodes sustainable and inclusive development. It is both a political and technical challenge. The U4 Anti-Corruption Resource Centre (U4) works to understand and counter corruption worldwide.

U4 is part of the Chr. Michelsen Institute (CMI), an independent development research institute in Norway.

www.u4.no

u4@cmi.no

U4 partner agencies

German Corporation for International Cooperation – GIZ

German Federal Ministry for Economic Cooperation and Development – BMZ

Global Affairs Canada

Ministry for Foreign Affairs of Finland

Ministry of Foreign Affairs of Denmark / Danish International Development Assistance – Danida

Norwegian Agency for Development Cooperation – Norad

Swedish International Development Cooperation Agency – Sida

Swiss Agency for Development and Cooperation – SDC

UK Aid – Foreign, Commonwealth & Development Office