# U4 Helpdesk Answer

U4 Helpdesk Answer 2021:23

# Illicit finance and national security

Illicit finance can be used by adversarial actors to conduct a range of hostile activities, such as interfering in another country's political system, evading sanctions, funding armed operations or laundering tarnished reputations.

Financial secrecy undermines a country's ability to pursue a coherent security and foreign policy strategy. The lack of beneficial ownership transparency, the under-regulation of political finance, as well as the limited enforcement and prevention of financial crime help facilitate illicit financial flows that weaken national security.

Policy responses to curb these illicit financial flows will have to start by addressing the gaps that are exploited by adversarial actors. This could include reforms that: strengthen beneficial ownership transparency, enhance the capacities of financial crime authorities, better regulate activities of foreign lobbyists, and create more substantive restrictions on political financing.

6 December 2021

**AUTHOR**

**Mathias Bak (TI)**

tihelpdesk@transparency.org

**REVIEWED BY**

**Sophie Lemaître (U4)**

**Tymon Kiepe (Open Ownership)**

**Matthew Jenkins, Jon Vrushi and Jorge Valladares (TI)**

tihelpdesk@transparency.org

**RELATED U4 MATERIAL**

↗ Links between illicit financial flows and peace and security

# Query

## How and where is illicit finance used by adversarial actors to undermine national security?

## Contents



**MAIN POINTS**

- The use of illicit finance to conduct hostile activities can be thought of as a hybrid threat.
- Illicit finance is used as part of foreign influence operations, targeting both politicians and more grassroots-level actors.
- Adversarial actors can exploit vulnerabilities in poorly regulated financial systems to finance more openly hostile activities, such as the proliferation of weapons, violent extremism, armed operations and organised crime.
- Efforts to counter the use of illicit finance by hostile interests will have to begin at home.
- Potential policy responses include legislation that improves beneficial

## Glossary

**Illicit financial flows.**

There is no universally agreed-upon definition of the term Illicit Financial Flows, but according to Global Financial Integrity, IFFs refer to 'money that is illegally earned, used or moved and which crosses an international border' (see Solomon 2019).

A more recent statistical definition developed by UNCTAD and UNODC holds that the term IFFs refers to 'financial flows that are illicit in origin, transfer or use, that reflect an exchange of value and that cross country borders' (see UNODC 2020:12).

**Strategic corruption.**

Strategic corruption is the use of corrupt means to increase influence and shape the political environment in a targeted country (see Zelikow et al 2020). In its most organised form, 'corrupt inducements are wielded against a target country by foreigners as a part of their own country's national strategy' (Zelikow et al 2020).

**Hybrid warfare.**

Hybrid warfare refers to overt or covert actions orchestrated by an adversarial actor which falls short of general armed conflict, but nevertheless seeks to undermine or threaten the safety and interests of a state, including: the integrity of its democracy, its public safety, social cohesion, reputation or economic prosperity (Dowse and Bachmann 2021). Means of hybrid warfare can include disinformation, cyber attacks, use of proxy groups, economic manipulation and strategic corruption (Dowse and Bachmann 2021; Splidsboel 2017)

**Adversarial actors.**
For the purpose of this paper, an adversarial actor can be any actor, state, or non-state, pursuing an objective which is in conflict with the national security of another country.

**National security.**
There are many competing definitions of national security. In this paper, national security is understood as the 'protection and safety of the political, economic and other interests and values of the state' (Injac 2016). Threats to national security can include those that undermine a country's 'status as a free and democratic society [arising] from unlawful acts or foreign interference' (New Zealand Department of the Prime Minister and Cabinet 2017).

# Introduction

In recent years, the potential of corruption as a foreign policy instrument has received increased attention. The introduction of concepts such as 'strategic corruption', which aim to capture the ways in which states use corrupt means to gain influence and power over their rivals and adversaries, have found their way into foreign policy debates1 (Zelikow et al 2020; Murray et al 2021; Walker 2018: 10).

The theory of hybrid warfare is a useful lens through which to analyse the relationship between strategic corruption, illicit financial flows (IFFs) and hostile activities. It encompasses a range of hostile activities that fall just below the threshold of conventional armed conflict, and that seek to subvert an adversary via a combination of hostile non-physical interventions (Dowse and Bachmann 2019). Typically, operations in hybrid warfare can include measures such as cyber attacks, disinformation campaigns, political assassinations, economic coercion and malign finance. Hybrid warfare is a low-cost means of making an enemy do what they otherwise would not, without having to resort to military force (Dowse and Bachmann 2019).

In 2013, Russian generals presented a military doctrine that promoted what would become known as a 'new generation of warfare'. It predicted that war would become increasingly hybrid in nature (Murray et al 2021; Splidsboel 2017: 4). While some analysts regard hybrid warfare as a novel development, so-called 'active measures' were a range of similar tactics were employed by the KGB as early as the 1980s. These methods were intended to clandestinely enhance Soviet influence through deceptions and misinformation (Kux 1985).

1 While the literature on strategic corruption has tended to focus on state actors, the role of non-state actors and other interest groups (that may be partly embedded in state organs) should not be overlooked. As described in this paper, foreign non-state actors often play a key role in perpetrating corrupt acts that threaten other countries' national security.

A concept of warfare that extends beyond military operations to include areas such as the economy, culture and political institutions has been a staple of Iranian strategic thinking for at least the last 40 years (Golkar 2012). Similarly, Harold et al (2021) argue that China's current operations to expand its influence abroad are based on a longstanding strategy of propaganda and hybrid warfare.

One of the primary challenges of determining whether certain corrupt acts can be viewed as instances of 'strategic' or 'weaponised' corruption relates to the need to establish the intentionality that these terms imply (Murray et al 2021). This point is critical, as there is often a lack of proof that corrupt schemes are orchestrated and coordinated by political leaders in pursuit of foreign policy objectives. Even if this intent does exist, it may be difficult to demonstrate and prove.

Nonetheless, debates over corruption and illicit finance as a tool of hybrid warfare now feature more prominently in political discourse.

For instance, Financial Times journalist Tom Burgis (2020), argues that there is an informal alliance of kleptocrats that are partly embedded in the organs of state in a number of countries that seeks to reconfigure power to their advantage and benefit. According to Burgis and others, this alliance is deeply entrenched in the global financial system, penetrating global financial centres and property markets. These networks have successfully penetrated the political establishments of western democracies by identifying and exploiting democratic vulnerabilities with the ultimate goal of cementing their own political advantage and systems (Burgis 2020).

Like Burgis, Hála (2020: iii) argues that authoritarian regimes have come to use what he labels 'corrosive capital' as a means of strengthening their influence globally. According to Hála, the use of such corrosive capital brings an additional advantage to authoritarian states, because its transnational nature means that it weakens political institutions in liberal democracies, their systemic rivals. Corrosive capital, Hála (2020: 1) claims, often seeks to co-opt key individuals, thereby capturing critical institutions. Walker (2018: 10-11) argues that authoritarian regimes project influence through more diverse channels than was previously the case – for instance by manipulating information streams. In this way, adversarial actors are able to leverage opportunities provided by globalisation to exploit the vulnerabilities of open democracies, influence political elites in foreign countries and sow discord in target societies.

In the political realm, the current President of the United States (US), Joseph Biden, has been among those who have brought new urgency to efforts to address the issue of strategic corruption, having repeatedly referred to it in his speeches and writings (Biden and Carpenter 2018). The current US administration has pledged to design a comprehensive response to tackle foreign malign influence (Biden and Carpenter 2018), and has begun developing a strategy for addressing the interference by kleptocrats in US foreign policy (Bellows 2021). In the summer of 2021, the White House officially released a memorandum framing corruption as a national security issue for the United States (White House 2021). The memorandum mentions the role of financial opacity as an enabler of such corruption, allowing for illicit wealth to be laundered (White House 2021). The use of finance as a means of gaining influence abroad has also been a subject of discussion elsewhere, including in Australia and

the European Union (see Parliament of Australia 2017)

However, strategic corruption is not exclusive to authoritarian regimes. Intelligence agencies from democratic countries have also used subversive (hybrid) tactics in support of their foreign policy objectives, including in Afghanistan (Lynch 2021; Schmeidl 2016; McGinty 2010) and Latin America (see Greentree 2015). For instance, Greentree (2015) argue that US foreign policy in Central America in the 1980s can be largely viewed through the lens of hybrid warfare. According to Greentree, the US worked to contain leftist revolutions via a range of clandestine policies that, for the most part, stayed below the threshold of what is conventionally considered to be warfare.

This paper examines how adversarial actors' illicit financial activities can threaten other states' national security. The next section will briefly outline what this entails.

## Definitions, concepts and caveats

There is no universally agreed-upon definition of the term Illicit Financial Flows (IFFs), but a widely recognised and approved definition has been provided by the UN Organisation Against Drugs and Crime (UNODC) and the UN Conference on Trade and Development (UNCTAD). According to this definition, IFFs are 'financial flows that are illicit in origin, transfer or use, that reflect an exchange of value and that cross country borders' (UNODC and UNCTAD 2020: 12). Another definition coined by Global Financial Integrity considers IFFs to be 'money that is illegally earned, used or moved and which crosses an international border' (Solomon 2019). In other words, illicit finance is money that is either dirty because of the nature of its source, the way it is transferred from one entity to another, the way it is spent, or a combination of the three. It is worth noting that the lines between what is illicit and licit can often be blurred, particularly when what is widely considered hostile may be perfectly legal. Money can be used for multiple purposes that fall on both sides of the law. For instance, money that has been successfully laundered (illicit and illegal) can later be used for foreign lobbying, which depending on how the lobbying is conducted and provisions of the domestic legal framework in the target country could possibly be considered illicit, but still be legal.

While the term 'hostile state activity' is gaining ground to refer to hostile actions perpetrated by foreign governments, particularly in the United Kingdom, this term can potentially be unhelpful. This is because it implies that the hostile action in question has been orchestrated and coordinated by a de jure state (i.e. a state with a seat at the United Nations). In many cases hostile acts may not be perpetrated directly by an adversarial state, but by non-state actors or non-state actors that have developed state-like characteristics (such as the Islamic State, which, at its peak, had many of the characteristics of a de-facto state). These non-state actors may either be acting in a corrupt or corrupting manner to further their own private interests (such as stashing ill-gotten gains in high value property markets abroad), or they may be doing so under the direction of other states. In other cases, it is difficult to prove beyond reasonable doubt that an attack was orchestrated at the state level. For this reason, this Helpdesk Answer employs the term 'national security threat' whenever possible, as this does not necessitate proof of intent, and it also encompasses hostile activities undertaken by a wider array of actors.

This paper focuses on three areas that demonstrate clear links between national security and illicit financial flows. More precisely, it examines three ways in which illicit finance can be used by adversarial actors in ways that can be considered hostile to third party states.

First, illicit finance can potentially be used as a means to interfere in an adversary's political life. Finance can be used to 'capture' influential or potentially powerful individuals to act – willingly or unwittingly – in the interest of foreign actors. It can also be used to exercise undue or illegal influence over democratic institutions or processes, such as by circumventing restrictions on political donations from foreign sources.

Second, illicit finance can be used as a means of reputational laundering or projecting soft power. Adversarial actors can also use ill-gotten gains to fund research, civil society organisations and think tanks to try and secure increased influence or run positive public relations campaigns. At times, the differences between these types of schemes are blurry.

Third, illicit finance can be used by adversarial players to evade sanctions, and/or finance combat operations, organised crime, violent extremism or attempts at proliferating weapons of mass destruction.

The paper does not focus on what could be termed 'geoeconomics', in other words the use of economic tools to advance geopolitical objectives (Schneider-Petsinger 2016). As such, discussions around the realpolitik of strategic investments, such as the Belt and Road Initiative, The Nord Stream pipeline, construction of 5G networks and other large infrastructure projects with major geopolitical implications fall outside this Answer's scope. Links between foreign investment in critical infrastructure and national security concerns appears to be more related to the control and ownership structures of the entities that are investing in critical sectors than the – potentially illicit – source, transfer or use of investment finance per se.

## Illicit finance and malign political interference by foreign actors

The first way in which foreign actors can use finance to obtain influence in target countries is using money to fund political activities in foreign countries. The intelligence community and civil society organisations in several democracies have documented how so-called 'active measures[2]' have extensively targeted prominent political players and networks, sparking questions over the extent of influence adversarial foreign states hold over political processes in these countries (Sutton and Clark 2020).

Rudolph and Morley (2020: 1) describe the financial part of such active measures as 'malign finance' – '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.'

Malign finance can work in a variety of ways, but often involves foreign states funnelling money into political processes in target countries (Rudolph and

2 Covert, hostile influence operations

**Cases of malign finance**

- Support towards the election of a pro-Russian, Eurosceptic German MP, who, according to leaked Russian documents, was under a high degree of political control (Gatehouse 2019).
- Loans made to France's Front National election campaign in 2014, allegedly in return for recognising Crimea as a Russian territory (Sonne 2018).
- Active measures extensively used by Russia in the 2016 US presidential election campaign (Mueller 2019). These reportedly included covert funding received by individuals close to former President Donald Trump (see Mueller 2019).
- Among those Russian oligarchs believed to have interfered in the 2016 US presidential elections were the aluminium tycoon Oleg Deripaska and Konstantin Kilimnik (US Treasury 2018).
- Long-standing concerns in the UK related to oligarchic sources of funding to a network of shell companies and charities that engage heavily in political financing (Alliance for Securing Democracy n.d.). These include a string of unclarified questions regarding the suspicious origin of some of the funds for the Leave.eu campaign, which reportedly held up to seven undisclosed meetings at the Russian embassy (Cadwalladr and Jukes 2018).
- Active measures by Russia outside of the Global North have been recorded in places such as Bolivia, where operatives have attempted to aid former President Evo Morales' attempt at re-election (Heldevang 2019).

Morley 2020: 1). Often this is an attempt to influence electoral outcomes; but in addition to funding political campaigns, foreign finance may also be used to pay for political advertisements or influence incumbents' policy positions outside of campaigning periods.

According to Rudolph and Morley (2020: 1), foreign actors approach individual targets and seek to form financial links. Based on their analysis of available cases and open-source intelligence, Rudolph and Morley arrived at the following breakdown of malign finance mechanisms employed: straw donors[3] (22%), various criminal means (17%), in-kind gifts (15%), non-profits (13%), companies (11%), online ads (11%) and online outlets (10%).

As noted above, while such transactions can further the interests of adversarial actors, they may not always be illegal, as the source of the money could be legal and the way the funds are transferred may not necessarily break any campaign financing law. Therefore, as detailed below in the section on potential policy responses, tightening up campaign financing laws is central to curbing undesirable foreign influence on domestic politics.

According to Rudolph and Morley (2020: 1), since 2016, actors linked to Russia, China, Iran and the United Arab Emirates have spent more than US$300 million to interfere in political processes in democracies via covert funding. Rudolph and Morley (2020: 1) have documented around 100 incidents of malign financing in 33 countries across the world. The number of such incidents has increased, and in the years following 2016, there have been approximately 15–30 cases of malign

3 A straw donor is a donor who hides the true origin and purpose of a political donation.

financing activities reported annually (Rudolph and Morley 2020: 1).

It should be noted, however, that these cases have been identified using only public sources, and it is likely they represent a small sample of the true incidence. Another major caveat with these numbers is that they only reflect financial involvement of non-NATO members, and therefore may exclude malign financing activities by NATO countries.

According to Rudolph and Morley, Russian-affiliated individuals are responsible for most of these interventions, followed by entities with connections to China, Iran and the United Arab Emirates (Rudolph and Morley 2020: 4).

However, such schemes do not target all countries equally. In Europe the two most affected countries, by a significant margin, are Ukraine, where illegal means are often used to interfere with political processes, and the UK, where there are a substantial number of cases involving straw donors (Rudolph and Morley 2020: 4).

China's financial involvement in foreign politics seems to be primarily based in democracies in its own neighbourhood. The cases of Chinese financial involvement in European and American politics – perhaps contrary to popular perception – appear quite modest in comparison with money of Russian origin (Seldin 2021). That said, covert finance has become a tool for Chinese interference in Taiwanese politics. Tycoons with ties to the Chinese Communist Party (CCP) have bought a number of media outlets, and some of these outlets have become increasingly aligned with the CCP, and occasionally spread CCP-aligned information (Kurlantzick 2019). Chinese propaganda in the 2020 Taiwanese elections reportedly backed the opposition, which in the past has been more open to the suggestion that Taiwan is a province of China (Kurlantzick 2019). In addition to Taiwan, Chinese influence operations are believed to be targeting the political systems of Australia and New Zealand (Walker 2018: 12).

## Illicit finance and influence operations at the grassroots level

While most of the discussion has been centred on how malign finance can be a means of infiltrating adversaries' political systems at the highest levels, evidence also suggests that politics can be influenced at the grassroots level.

One of the initiators of Occupy Wall Street, a protest movement that formed in response to the global financial crisis, claims that Russian intelligence services attempted – albeit unsuccessfully – to co-opt the movement (White 2017). According to White (2017) the attempt by foreign adversarial intelligence operatives to co-opt Occupy Wall Street is emblematic of a larger issue: the attempt to tap into and obtain influence over social movements in foreign countries. This is allegedly a counter-strategy to what Russia reportedly perceives to be similar tactics deployed by Western states in the 'colour revolutions' in Europe's Eastern Neighbourhood region and during the Arab Spring (White 2017).

This strategy has evolved in recent years. According to White (2017), Russian intelligence appears to be increasingly attempting to establish groups that mimic legitimate social movements in other countries. White (2017) recounts an encounter with someone purporting to represent a group called 'Black Matters' in a clear attempt to appear affiliated with the Black Lives Matter protests. It was later discovered that 'Black Matters' and other

fake activist groups appear to have been were set up or funded by Russian operatives seeking to sow discord in the United States (Levin 2017). The concern is that people may end up directly or indirectly supporting these movements without knowing the funding structures or 'beneficial owners' of these copy-cat organisations (White 2017; Švedkauskas 2020).

In the Baltic countries, pro-Russian NGOs that, according to Lithuanian intelligence, 'discredit the Baltic states internationally and encourage ethnic disharmony at home', frequently obtain funding (Alliance for Securing Democracies, n.d.). One example involves an organisation called World Without Nazism, which has been described as a Russian influence operation by the Latvian intelligence services, and has received substantial funding from Russian backers (Alliance for Securing Democracies, n.d.).

In much of mainland Europe, Turkey has funnelled significant amounts of money to organisations that strengthen the influence of the ruling Justice and Development Party (AKP), and Nationalist Movement Party (MHP). Often described as one of the key elements of Turkey's 'long arms in Europe', the Milli Görüş movement, a Turkish Islamic-Nationalist organisation, boasts around 300,000 members in Europe (Vidino 2017). Milli Görüş is largely funded as a 'religious endeavour' via Diyanet, the Turkish Directorate for Religious Affairs, whose aims and administrative structures are becoming increasingly blurred. Most Milli Görüş activities are not necessarily extremist and the organisation is not openly violent. However, some of the financial flows from Turkey are funnelled into an extensive network of private associations that reportedly mobilise members to conduct surveillance on, and sometimes kidnap or attack political opponents of the incumbent government, particularly members of Fethullah Gülen's movement, or activists who advocate for minority rights (Vidino 2017). According to Vidino (2017) these efforts are coordinated by the National Intelligence Organisation in Turkey (MIT) or by individuals embedded in Turkish embassies.

Turkey's 'long arms' are believed to stretch relatively far into countries such as Germany, with a number of Turkish civil society organisations reportedly being funded and coordinated by the AKP (Pieper 2018). Across Europe, there have been reports of political parties' links to Turkey, including concerns from Sweden and the Netherlands about Turkish influence in the political process (Norell 2020).

## Influence operations via organised crime

Turkish illicit finance has also flowed into organised criminal organisations. For instance, both MIT and AKP have allegedly employed the use of mafia-style groups and criminal gangs to assassinate or violently assault opponents abroad (Winter 2017). According to Winter (2017), in one case from 2017, a biker club known as Osmanen Germania was funded by an AKP parliamentarian to assault 'terrorists', Kurds, and people who advocated for Germany to acknowledge the Armenian Genocide. The money was allegedly handed out in cash directly by the AKP parliamentarians in question (Winter 2017). This is but one case in an established pattern of coordination between organised crime and actors embedded in the Turkish state who have sought to project influence abroad (Global Initiative 2021; Bellut 2021).

A related issue, which generally plays out in more fragile states, is that of private charities'

'chequebook diplomacy' (Al-Shebabi 2017). Chequebook diplomacy refers to the spending by individuals and government entities with powers to undertake off-budget discretionary spending with the goal of building influence abroad (Al-Shehabi 2017). For instance, according to Al-Shebabi (2017) a significant amount of Qatar's foreign policy spending is off-budget, unaccounted for, and at the discretion of private entities ( see alsoMeester et al 2018: 1). Qatar has been accused of sponsoring political parties and armed movements in Afghanistan, Syria, Mali, Algeria, Tunisia and Libya (see Reuters 2017; Al Shebabi 2017).

According to Gartenstein-Ross and Zelin (2013), some large charities based in the Gulf transfer funds under the guise of humanitarian aid, but it is suspected some of these monies end up in the hands of extremist groups. One ongoing case filed in London involves allegations levelled against Qatari state-affiliated actors that they transferred substantial sums to the Nusra Front (Weinthal 2021).

## Reputational laundering

Another form of the illicit use of finance in ways that could be harmful to other states' national security is 'reputational laundering'. Reputational laundering 'is the process of concealing the corrupt actions, past or present, of an individual, government or corporate entity, and presenting their character and behaviour in a positive light' (Comsure Group 2016).

While a country seeking to bolster its image abroad may not sound on the surface to be a potential threat to national security, the examples below illustrate that such an agenda can be linked to attempts to undermine the independence of the judiciary, the rule of law or the legislative process in target countries, as well as seeking to infiltrate the media landscape.

Corrupt or adversarial actors can engage in reputational laundering in a variety of ways, including through the use of dubious lobbying practices. As described in the section below, an increasingly common way of engaging in reputation laundering is by investing in sports clubs.

One illustrative case of reputational laundering is that in which Azerbaijan bribed 13 members of the Parliamentary Assembly of the Council of Europe (PACE) in an effort to stifle criticism by PACE of Azerbaijan's human rights conduct (Chase-Lubitz 2018). One member of PACE received €25,000 from a company based in the UK implicated in a money laundering case investigated by The Organized Crime and Corruption Reporting Project (OCCRP) (Chase-Lubitz 2018).

In a report on foreign lobbying in the UK parliament, Transparency International UK (2018: 3) argued that 'the activities of the Azerbaijan lobby in Parliament have become so infamous that it is seemingly tolerated as almost an eccentricity'. These activities raise concerns that parliamentarians may help to legitimise the influence of Azerbaijan or in extreme cases represent Azerbaijani rather than UK national interests (Transparency International UK 2018).

Pevehouse and Vabulas (2019) claim that, overall, this kind of lobbying can influence a country's foreign policy, noting that there is a statistically significant correlation between the scale of lobbying by foreign states, and desirable foreign policy outcomes for those states. All else being equal, an increase in foreign lobbying (as measured in dollars spent) leads to more favourable US

assessments of the human rights situation in that country when compared to previous years and more objective indices (Pevehouse and Vabulas 2019: 85). Therefore, extensive lobbying by foreign actors can help shape a country's policies and attitudes towards other states.

In the US alone, the amount of money spent on lobbying by registered foreign agents since 2016 stands at US$2.3 billion. This is almost as much as the US$2.4 billion spent in the 2016 presidential election (Seely 2021: 3).

One of the best and most revealing examples of this lobbying is Turkish lobbying in the US (Pevehouse and Vabulas 2019:85). Turkey reportedly has a long-standing lobbying infrastructure of PR firms, Ankara-connected charities and lobbyists to target politicians and key individuals (Klasfeld 2019). In the US, the Turkish lobby has long been one of the most active and secretive foreign lobbies (Klasfeld 2019; Bjorklund 2021). While some of these lobbying efforts are disclosed to the Department of Justice, there are cases where money has found its ways to key politicians in murky and undisclosed ways. For instance, money has been channelled via US-based Turkish charities reportedly affiliated with members of the Erdoğan-family and via secretive companies (Klasfeld 2019).

Working through various subcontractors, according to Klasfeld (2019), Turkish actors have been able to influence several US lawmakers to represent Turkey in a positive light. In one instance, lobbyists working on behalf of Turkey sought to stop a court case in the US, in what is considered the largest sanctions evasion case in history (Bjorklund 2021). In another case, Turkey was able to influence several politicians to support efforts to have Fethullah Gülen extradited, under the guise of the so-called 'Truth Campaign' (Klasfeld 2019).

Opaque corporate structures play a key role in obscuring funding sources used to try and influence other countries' foreign policy. For instance, a Dutch company whose beneficial owners, according to Klasfeld (2019), are Turkish, reportedly paid former National Security Adviser Michael Flynn US$600,000 to write an op-ed in which he compared Gülen to Osama Bin Laden.

## Sportswashing

Reputational laundering also extends to high-profile cultural activities, such as sport. This has given rise to the term 'sportswashing' (Doward 2018), which denotes reputational laundering through sports. Many Premier League football clubs, for instance, have reportedly received cash flows from anonymous individuals who may in some cases be investing in football clubs as a means of laundering dirty money (Harrison 2021) or dirty reputations (Doward 2018). This is possible because using offshore trust accounts allows an individual to conceal one's true identity, and thus easily bypass checks that have been put in place by the authorities (Harrison 2021).

Two prominent recent cases of sportswashing include the takeover of Newcastle United by Saudi Arabia's Public Investment Fund (Conn 2021), as well as the decision to award Qatar the 2022 FIFA World Cup (Gibson 2015). Indeed, Qatar's bid was characterised by serious irregularities, with several allegations of corruption levelled against senior-level officials involved in the bidding process. Out of 22 officials involved in the bidding process, 16 have been criminally charged (Strøm 2021) and some of those who were involved in the process

have admitted that their vote for nominating Qatar was paid for (Laughland 2017).

## Sanctions evasion

In addition to using illicit finance as a means of obtaining influence in foreign countries, adversarial actors can exploit vulnerabilities in poorly regulated financial systems to finance more openly hostile activities, such as proliferation of dangerous materials – ranging from small arms to nuclear or chemical weapons – violent extremism, armed operations and organised crime.

North Korea is among the most sophisticated actors when it comes to exploiting vulnerabilities in the global financial system to evade sanctions. In recent years, North Korean hackers have successfully penetrated a number of financial institutions. One prominent case involved North Korean agents stealing an estimated US$81 million from Bangladesh's central bank, then laundering this money through casinos in other Asian countries (Rosenberg and Bhatiya 2020). North Korean hacker groups have also infiltrated ATMs and firms around the world, and have built sophisticated systems to steal and sell sensitive data and industrial secrets (Rosenberg and Bhatiya 2020). The proceeds of these endeavours could potentially be used to fund the country's missile programme (Rosenberg and Bhatiya 2020).

This industrial-level cybercrime relies on the sophisticated use of money laundering and sanctions evasion, and webs of anonymised shell companies leading back to ever changing front men that can easily move addresses and change identities. By the time compliance professionals have done their due diligence and 'know your counterpart' (KYC) checks, or investigators discover a scheme, ownership structures have changed or a new front man is in charge (Rosenberg and Bhatiya 2020). Simply put, the current regulatory regime and lack of beneficial ownership transparency requirements affords North Korea a level of versatility that allows it to evade sanctions with impunity. In one recent case, North Korean businesses with links to the North Korean government were able to win several large-scale government contracts in the Democratic Republic of the Congo (the Sentry 2021). Investigations conducted by the Sentry (2021) demonstrated how these businessmen had enjoyed access to the global financial system via a US dollar account at the Cameroon-based Afriland First Bank and a web of proxies (the Sentry 2021).

The Iranian regime has also been able to evade comprehensive sanctions. In one case, a bank affiliated with the Islamic Revolutionary Guard Corps (IRGC) escaped sanctions using a network of front companies in the United Arab Emirates and Turkey in order to access foreign currency. By employing networks of front businesses, the IRGC was able to inject money to fund Quds Forces operations in the region (Talley 2019).

Similarly, in what is known as the 'gas for gold' scandal, the Turkish state-owned Halkbank, and top Turkish government officials, assisted Iran in evading sanctions in relation to transactions worth US$20 billion between 2012 and 2016. Bribing top government officials via this scheme, Iran was able to convert oil and gas revenue into gold in Turkey. The scheme was initially halted in 2014, then initiated again after a number of well-placed bribes to officials from the AKP (Bjorklund 2021).

Hezbollah is another organisation that has proven adept at capitalising on various loopholes in financial markets. In fact, the group has become so professional at handling dirty money, it has

reportedly built a global money-laundering, terrorist financing and sanctions evasion operation, stretching from the Middle East to West Africa, Latin America and into the United States and Europe (Ottolenghi and Badran 2020). In one recent case, a Hezbollah operative moved a significant amount of drug money for Latin American cartels, using a global network of 'thousands' of companies and financiers engaged in trade-based money laundering schemes, and trading at small volumes or practicing trade misinvoicing (i.e. over invoicing or submitting fake invoices) (Ottolenghi and Badran 2020).

These entities used the regular banking system (including in western countries) to undertake transactions, and generally were able to fly under the radar. It is believed that Hezbollah finances its operations, in part, via commissions on laundering money for organised criminals (Ottolenghi and Badran 2020).

Like North Korea, Iran and Hezbollah, the Syrian regime has also circumvented sanctions with relative ease by using well-known financial loopholes and a network of offshore shell and front companies. In one case, according to leaked files from the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), Syrian regime-linked individuals transferred money via Turkish petrochemical companies and the Bank of New York Mellon to a Malta-registered company called Petrokim to evade sanctions (Hille 2020). In mid 2020 Rami Makhlouf revealed that he had helped his cousin, Bashar Al Assad, evade sanctions by setting up a web of offshore entities (Moskowitz 2020). The revelation came as retaliation for Assad's alleged investigation into Makhlouf's business empire (Moskowitz 2020).

Venezuela is another country where corrupt individuals have been able to transfer illicit wealth through secrecy jurisdictions, thus escaping comprehensive sanctions. Initially, Venezuela's response to sanctions imposed by the US was to make a deal with a Mexican business association to exchange oil for basic necessities (Lafuente et al 2021). However, over time, this setup expanded into a scheme involving a vast network of financial intermediaries and shell and shipping companies stretching across more than 30 countries (Lafuente et al 2021).

Generally, lax regulations and inadequate beneficial ownership transparency helps facilitate the evasion of sanctions. In particular, real estate markets are often key channels for sanctions evasion schemes. The open-source intelligence analytics firm C4ADS (2018) has explored how real estate markets in Dubai enable evasion of sanctions. The study identifies 44 properties belonging to sanctioned individuals, as well as an additional 37 properties connected to organisations such as the Altaf Khanani Organisation, the IRGC, Hezbollah, various Mexican cartels, and key Syrian regime insiders such as Rami Makhlouf (C4ADS 2018: 3). The issue, however, is larger than these 44 cases; there are tens of thousands of dubious real estate transactions annually (C4ADS 2018: 57).

While Dubai's real estate sector has long been identified as a high-risk sector in a high-risk jurisdiction, it is far from being the only region implicated in such activities. Purchasing property through anonymous shell companies without having to go through enhanced due diligence checks, enables adversarial actors to evade sanctions and/or launder the proceeds of crime in cities such as London, Paris and New York (Martini 2019: 5).

In one case from New York City, a New Jersey-registered front company whose beneficial owners were Iranian regime insiders owned a 36-story skyscraper on Manhattan's 5th avenue. Investigators involved in the seizure of the property later found that Iranian politically exposed persons had been able to use the US property markets as far back as 1995 (Global Witness 2014: 7). In another case involving Iranian regime-affiliated individuals, an Iranian national invested a substantial amount of illicitly obtained wealth into at least six properties in California (Kim 2018). The person in question had set up a structure of linked shell companies that he used to facilitate transfers from the Government of Venezuela to an Iranian holding company. Some of the proceeds from facilitating this sanctions evasion scheme were re-invested into real estate (Kim 2018). In yet another case, high ranking officials in Venezuela's state-owned oil company used real estate to launder their money via anonymous shell companies (Global Witness 2020). According to Global Witness (2020) these individuals owned 12 apartments in Florida and Panama.

According to the UK 2020 national risk assessment of money laundering and terrorist financing, the London property market continues to be an attractive destination for illicit funds. It is estimated that a minimum of £ 5 bn in UK property has been acquired with suspicious funds (HM Treasury and Home Office 2020: 83). In a study of over 400 UK-based money laundering cases, Transparency International UK (2019: 4-5) finds that the leading countries of origin of dirty money include China, Russia, Nigeria and Ukraine.

Canadian cities also demonstrate how property in great cities are susceptible to exploitation by potentially malign actors. Analysing more than 1,4 million real estate transactions in the Greater Toronto Area, TI Canada found that CD $ 9,8 billion in real estate has been acquired through cash purchases from mostly anonymous companies with limited due diligence checks (Ross 2019). In addition to this, an unknown, but presumably substantial, number of purchases have been made through nominees, trusts and front companies (Ross 2019: 4).

When it comes to concerns about how terrorist-designated groups can exploit poorly regulated financial and real estate markets, Turkey is a prime example. When the Financial Action Task Force (FATF) grey-listed Turkey in November 2021, it expressed concern over the level of access that terrorist-designated groups have to the country's financial and real estate sector and how this allowed violent extremist groups, including ISIS and Al Qaeda to launder proceeds (Spicer 2021).

In the European Union, real estate has been used to launder proceeds of crime, corruption or terrorism in countries including the Czech Republic, France, Greece, Finland, the Netherlands and Portugal (Remeur 2019).

Current regulatory standards in most countries enable these sanctions evasion practices, creating a situation in which actors involved in illicit finance related to corruption, transnational organised crime and violent extremism have unfettered access to financial and real estate markets in democratic states. Harrison and Gyenter (2020) frame this paradox as if 'during the height of the Cold War, representatives of Soviet KGB chief Yuri Andropov strolled down K Street in downtown Washington, DC, to shop for a lobbyist, a PR agency, and a lawyer'.

Leaks such as the 2020 FinCEN files have demonstrated that kleptocratic regimes, organised

criminals and violent extremists have, with relative ease, exploited lax regulations to conceal malign financial transactions via key global financial systems. The FinCEN files contained explosive information about the players that exploit western countries' financial systems. However, containing information on only 2,100 out of 12 million Suspicious Activity Reports (i.e. 0.02%), the FinCEN files are but the tip of the iceberg of what goes on in the world of illicit finance (Lynch 2021).

# Potential policy responses

There is widespread agreement that efforts to counter the use of illicit finance by adversarial players in ways that undermine national security will always have to begin at home, especially in jurisdictions that see large-scale inflows of dirty money (Keatinge et al 2021).

## Beneficial ownership transparency

Drawing on recommendations made in the available literature, the first possible policy response that many analysts consider is establishing regulation that makes beneficial ownership structures more transparent. It is widely believed that access to up-to-date information on the true owners of a company is crucial for law enforcement, intelligence agencies, and supervisory and tax authorities to do their work. Currently, the system of collecting such information is patchy at best, as while some countries have begun to implement reforms, others lag behind.

Organisations such as Transparency International (TI) (2021), Global Witness (2020), Basel Institute of Governance (2021), Extractive Industries Transparency Initiative, among many others, have called for a number of reforms to current systems of beneficial ownership disclosure, in order to create better systems for countering illicit financial flows. These reforms also have the potential to curb the use of illicit finance in ways that are detrimental to states' national security.

First, beneficial ownership transparency advocates call for states to establish centralised, publicly-available, beneficial ownership registers (TI 2021; Open Ownership 2020). These registers, advocates contend, should be open to the public to allow for better international cooperation between intelligence and law enforcement, and to enable journalists and civil society to assist in the discovery of irregularities (Transparency International 2021). In order to be effectively implemented all companies should have reporting obligations towards this register, including non-financial gatekeepers (such as lawyers, accountants and real estate agents).

Currently, many authorities (including financial intelligence units and financial crime investigators) rely on financial institutions and firms dealing with high-risk clients, such as lawyers, accounting firms and real estate agents, to disclose suspicious activity discovered during due diligence (DD), KYC, and 'know your counterpart's counterpart' (KYCC) procedures (Martini 2019: 3). This system is not fit for purpose for many reasons, including financial institutions' inadequate compliance and DD procedures, and simply due to inaccurate or outdated data.

Furthermore, proponents of beneficial ownership transparency argue that ownership data should be verified independently and kept up to date. This includes recording the ID, address, nationality and other key information of shareholders and directors (Transparency International 2021).

Policymakers should also consider addressing particular loopholes used to layer dirty money into the legal economy. For instance, bearer shares, which are physical certificate shares with no name attached (indicating the ownership of whoever carries it), allow for a substantial amount of secrecy and anonymity. This enables criminals, terrorists or politically exposed persons to transfer companies and assets outside the purview of any regulatory body. Bearer shares, Transparency International (2021) argues, should either be banned or have regulatory requirements attached to them in order to allow financial crime investigators to identify any criminals using these methods.

The use of nominees is another frequently used means to maintain financial secrecy. Nominees typically act on behalf of an owner who wishes to remain anonymous. The practice is legal, but is frequently exploited by adversarial actors. These loopholes can be closed if regulation governs who can be a nominee (e.g. only lawyers or accountants can be nominees) and obligates nominees to disclose on whose behalf they are operating (Transparency International 2021).

According to advocates for beneficial ownership transparency, it is also crucial that governments apply the same beneficial ownership rules to foreign companies that they apply to domestic ones. In some cases, rules for disclosure are laxer for foreign companies than for domestic ones (Transparency International 2021). There are nonetheless challenges when it comes to verifying disclosures of foreign entities, and conversations with experts conducted for this paper indicate that the best outcome is likely to be the integration of interoperable, machine-readable national registers to gain visibility of transnational ownership structures.

A useful resource for those exploring policy responses to counter illicit finance is the Open Ownership Principles (OO Principles), which comprise nine principles for beneficial ownership transparency. The principles include:

1. There should be a clear legal definition of what defines beneficial ownership. A beneficial owner should always be a person, and third parties, nominees or intermediaries should not be able to register as beneficial owners (Open Ownership 2021: 3). Low thresholds for ownership (ownership shares) should be used for high-risk sectors.

2. Publicly available ownership data should cover all relevant entities, and exemptions should be provided only for those entities whose data can be found through other mechanisms (Open Ownership 2021: 4).

3. Beneficial ownership data should contain sufficient information on the beneficial owner, the declaring company and structures of ownership, so that the data can be interpreted and analysed accurately (Open Ownership 2021: 5).

4. Data should be provided in a single, standardised register (Open Ownership 2021: 7).

5. Access to beneficial ownership data must be public. Law enforcement, civil society, the private sector, media and citizens should have access to information. The private sector, in particular, can benefit from better and easier access to third party due diligence data (Open Ownership 2021: 8).

6. Beneficial ownership data must be structured and available for use on standard computer systems (Open Ownership 2021: 10).

7. Ownership data should be accurate and independently verified (Open Ownership 2021: 11).

8. Beneficial ownership data should be regularly updated. Submission windows should be relatively short. Historical ownership data should also be kept (Open Ownership 2021: 12).

9. There should be sanctions for non-compliance and these should be enforced in a proportional manner to deter actors from not complying (Open Ownership 2021: 13).

In addition to the nine principles, Open Ownership has also created a guide to implementing beneficial ownership transparency.

## Enforcement and prevention

While beneficial ownership transparency is a key, fundamental step towards a more coherent approach to financial crime, it is not enough in and of itself. Authorities and agencies with the mandate to tackle financial crime also need to be strengthened and, in many cases, require considerably more resources.

FinCEN, which has a staff of just 300, is one example of an under-resourced agency. These 300 employees are expected to follow up on no less than 5 million Suspicious Activity Reports (SARs) annually (Vittori 2021). Analysts have argued that where financial intelligence units (FIUs) lack resources to analyse even the most critical SARs, it is essential to substantially strengthen their capabilities (Vittori 2021). In other cases, such as the UK, the institutional setup for countering illicit financial flows is fragmented, with numerous bodies responsible for different aspects of tackling dirty money. In such cases, differing priorities, standards and strategies may undermine the enforcement of money laundering regulation (Keatinge et al 2021; Putze 2020).

Strengthening FIUs, other financial crime agencies, and the general institutional framework for countering and preventing financial crime is particularly important given the opportunities provided by new technologies, such as cryptocurrencies, and old, well-known, means of moving dirty money, such as hawala couriers. Both crypto and hawala are frequently used in the financing of terrorist activities or violent extremist groups (Davis 2021: 2).

Observers have also pointed out that supervision and regulation need to be extended to designated non-financial businesses and professions (DNFBPs), such as lawyers, accountants, corporate service providers, and real estate agents, who often act as enablers in the laundering of dirty money (Rahman 2021: 1). Currently, the system for supervising DNFBPs is considered uneven and inconsistent across jurisdictions, thus weakening the response of many countries to the challenges posed by DNFBPs (Rahman 2021: 1). Experts have argued that DNFBPs need better knowledge of how to implement adequate due diligence procedures, and they should be subject to significantly more supervision (Basel Institute on Governance 2021a).

According to Rudolph (2021) this is particularly pressing in the 'five great enabler nations' (the US, Australia, Germany, Switzerland and the UK), where the role of DNFBPs in facilitating corruption is extensive and regulation and enforcement can be patchy. Efforts to strengthen regulation of DNFBPs are underway. For instance, in the US, Congress is currently negotiating the Establishing New Authorities for Business Laundering and Enabling Risks to Security (ENABLERS) Act. The

ENABLERs Act extends due diligence requirements that are currently in place for banks to DNFBPs (US Congress 2021).

In addition to enforcement, many jurisdictions are doing little in terms of proactive steps to prevent money laundering and the financing of terrorism. According to the Basel Institute on Governance (2021b) AML index, jurisdictions are generally less effective at preventing illicit finance than enforcing rules. Ways to improve prevention, include introducing better policies and better risk assessments, setting up supervision structures, and requiring more due diligence measures (Basel Institute on Governance 2021b).

## Countering illicit finance and undue foreign influence in political life

A paper by the Organization for Security and Co-operation in Europe (OSCE) on third-party financing risks recommends that all countries in the OSCE require authorities to conduct assessments of the extent, effect and impact of involvement of foreign third parties in political activities, particularly around elections (Ohman 2020: 1).

Kergueno and Vrushi (2020: 32) recommend that third parties with political aims and activities ought to be subject to the same campaign financing rules as domestic political actors. This includes similar, or stricter limitations on electoral campaign expenditure, and clear rules on financial disclosure (Kergueno and Vrushi 2020: 32).

According to Ohman (2020) legislation to limit or regulate potential third-party involvement should delineate the specific financing activities to be targeted; set out concrete reporting requirements; and also ensure that there are measures in place when regulation is circumvented by either the receiver or sender of the funds. According to this view, it is also critical that regulation of foreign campaign financing is followed by concrete guidance for those who wish to receive such funding while adhering to the rules and norms of integrity in political financing.

Moreover, according to experts, regulation should be backed up by a strong oversight function that should be conducted by a politically and functionally independent, and adequately resourced institution (Ohman 2020: 1). Such an institution should not merely monitor compliance with existing regulations, but enforce sanctions when regulations are violated (Ohman 2020: 36). To confront foreign interference, it is recommended that the institution conducting this oversight must also enforce appropriate financial reporting standards.

Among TI UK's recommendations for avoiding conflicts of interests among parliamentarians is to set up independent monitoring of the conduct of parliamentarians (in the UK through the Parliamentary Commissioner for Standards) to assess whether MPs have ties with foreign adversarial or corrupt actors (TI UK 2018: 3). TI UK also recommends that politicians are advised on conducting better due diligence when travelling abroad or working with foreign lobbies (TI UK 2018: 3). Potential measures also include setting limits on the amount foreign governments or foreign entities can spend in terms of travel. According to TI UK (2018: 4), it is critical that the financial interests of any politician be disclosed through a system that is actually fit for purpose and gives the public insight into their financial dealings with foreign entities.

An outright ban on foreign donations to political actors can also be considered. This was the recommendation from a 2017 report on foreign election finance in 2016 Australian elections from the Australian Parliament's Standing Committee on Electoral Matters (Parliament of Australia 2017). A ban, the report argues, is the most feasible way to create a system with as few loopholes as possible. Indeed, a ban on foreign financing to political parties is relatively common globally, with many democratic countries considering such bans a standard protection of national sovereignty. Sixteen EU member states currently ban foreign political financing (Valladares n.d.). However, without increased beneficial ownership transparency, there are a number of loopholes that can be used against a ban, as the ultimate beneficial owners (UBOs) of entities that make donations remain unknown.

One major weakness is the use of a third party as a channel to circumvent financing rules (Valladares n.d.). This can be avoided, for instance, by defining these groups as 'groups that pursue election or referendum outcomes' and subjecting them to the same campaign financing rules as other political actors subject to regulation. Another loophole often exploited is the use of financial institutions as lenders to political parties or candidates. Loans can exchange hands several times, and sometimes end up being controlled by foreign interests. This is difficult to prevent, but, in addition to monitoring party financing, can be tackled by creating incentives for parties and candidates to look for funding through more transparent means, without seeking donors outside the country (Valladares n.d.).

## Controls on political advertisement

A related area of policy responses is to improve regulation of online political advertisements. The increased use of social media campaigns, with all the opportunities that entails, such as microtargeted ads, has come with dramatic changes to political processes. Many countries are ill-prepared for regulating the effects of these changes, with political financing rules that often do not adequately address the risks to an accountable and transparent political process (Dunčikaitė et al 2021: 1). These risks often manifest in targeted misinformation or disinformation campaigns, with damaging political consequences (Dunčikaitė et al 2021: 10-11). Moreover, unregulated microtargeting can create an 'arms race' of potentially untraceable ads (Dunčikaitė et al 2021: 12).

In the absence of regulation and transparency, foreign adversarial actors frequently conduct political influence operations, for instance by investing into channels that spread mis/disinformation or divisive content (Dunčikaitė et al 2021: 1).

Dunčikaitė et al (2021: 1) argue that online ads need to be better regulated if these vulnerabilities are to be addressed. Platforms that provide online political ads could be required to undertake some form of due diligence, including checking the authenticity of content, and basic KYC protocols. Further rules for the use of private data in microtargeting should be implemented (Dunčikaitė et al 2021: 2).

## Lobbying transparency

Increasing lobbying transparency is also a potentially effective policy response to safeguard

the integrity of national political processes against malign foreign influence.

One well-known model for monitoring the activities of foreign lobbyists is the US Foreign Agents Registration Act (FARA), which requires foreign lobbyists to register their work. Recently, Australia adopted the Foreign Influence Transparency Scheme (FITS) Act, which has been modelled on FARA (Seely 2021: 1). Many countries, however, have implemented legislation that does not cover all lobbyists acting on behalf of foreign countries (Seely 2021: 1).

It is important to note that such laws can and have been exploited to limit civil liberties and the autonomy of civil society organisations. This has been seen in Australia, for example, where FITS sparked a campaign called 'hands off our charities'. Such registration schemes for foreign agents need to be carefully designed so as not to unduly burden legitimate civil society organisations.

The International Standards for Lobbying Regulation (Lobbying Transparency 2015) established 38 standards as benchmarks for current best practice in lobbying transparency. Selected standards include, first and foremost, creating a lobbying register that clearly designates: the lobbyist's identity and the ultimate beneficiary of the lobbying practice; the subject matter of lobbying; lobbying expenditure; sources of funding; and potential political contributions (Lobbying Transparency 2015: 6; Kergueno and Vrushi 2020: 32). Measures to better capture the legislative 'footprint' could include mandatory disclosure of information on meetings between lobbyists and policy-makers alongside information on the legislation being discussed (Kergueno and Vrushi 2020: 32).

According to both Kergueno and Vrushi (2020: 31) and the Lobbying Transparency Principles (2015: 12), lobbying practices should be subject to oversight by an authority capable of investigating non-compliance as well as imposing sanctions when lobbying rules are violated. If it is to have the intended effect, such an authority should have a mechanism where violations against lobbying rules can be reported (Lobbying Transparency 2015: 12).

According to Lobbying Transparency (2015: 7), public access to information laws should also include guaranteed access to information about lobbying. Such information may include data on political finance and lobbying activities, as well as politicians' registered assets (Kergueno and Vrushi 2020: 31). The quality of data needs to be high enough for it to be useful in practice (Kergueno and Vrushi 2020: 31).

Additionally, a number of rules and guidelines for the conduct that is expected from both lobbyists and officials, including guidance for gifts, ought to be provided.

Finally, it is argued that resilience to foreign influence operations could be strengthened through stronger procedures for monitoring potential conflicts of interest among lawmakers, and with rules that regulate the practice of 'revolving doors' (Lobbying Transparency 2015: 8).

## National security investment screening

In 2009, the OECD issued its *Recommendation of the Council on Guidelines for Recipient Country Investment Policies relating to National Security*, which was intended to 'help governments maintain fair treatment of international investors while meeting their countries' security needs' (OECD

2009). While the recommendation set out certain principles of non-discrimination, transparency of policies, predictability of outcomes and proportionality of measures, it did not specify what investment screening checks might look like in practice.

More recently, in the last couple of years, several OECD countries introduced new investment screening regimes for foreign direct investment (FDI). These are generally aimed at safeguarding critical national infrastructure from potentially malign actors and to detect investments driven by non-commercial incentives (Lenihan 2021). Investments that could potentially undermine national security include investments driven by underlying motives such as espionage, facilitation of crime, terrorism or corruption, collection of sensitive data or investments that give foreign actors leverage over critical supply chains or important infrastructure such as health facilities.

As such, while these types of screening mechanisms are primarily intended to assess the potential security impact of legitimate investments into critical sectors, these type of background checks may have some potential use in identifying any illicit financial activity associated with proposed investments.

For instance, in spring 2021, Canada passed the Investment Canada Act and issued regulations and guidelines on reviewing investments' national security implications. The Investment Canada Act sets out a variety of entities that are subject to national security reviews, including Canadian businesses being acquired. Prior to an investment undergoing such a review, potential cases are referred to authorities by the relevant industries. The actual review is carried out by a number of relevant investigative bodies, including intelligence services, who look at the nature of the assets (Government of Canada 2021). Among other considerations, the Act stipulates that authorities are entitled to reject proposed investments in cases where the investment could potentially 'involve or facilitate the activities of illicit actors, such as terrorists, terrorist organisations, organised crime or corrupt foreign officials' (Government of Canada 2021).

Like the Canadian Act, the Danish government has approved a mandatory approval mechanism for FDI above a certain threshold value in selected sectors. The Danish Investment Screening Act is slightly different in the sense that the screening regime checks for both the threats to national security and public order, the latter of which the Danish law defines as the integrity of independent and democratic institutions (Gjøl-Trønning and Gall 2021).

Another two countries which have introduced similar schemes are Slovakia and the UK. Slovakia's Critical Infrastructure Act obligates companies operating in critical sectors to inform and receive approval from the government if they see a change in the ownership structures and introduces national security screening in critical sectors (Skoumal et al 2021).

The UK's National Security and Investment Act appears to be broadly similar, in that significant FDI and acquisitions in sectors of importance to national security have to undergo a screening process. The Act also introduces a number of sanctions for non-compliance, such as fairly substantial fines and custodial sentences (Hall 2021).

# References


Alliance for Securing Democracy. n.d. Malign Finance Tracker.

Al-Shehabi, O. 2017. Show Us the Money: Oil Revenues, Undisclosed Allocations and Accountability in Budgets of the GCC States. London School of Economics Kuwait Programme Paper Series: 44.

Basel Institute on Governance. 2021a. Money laundering risks: are we paying enough attention to lawyers, accountants and others beyond the financial sector? Basel AML Index, September 27.

Basel Institute on Governance. 2021b. How effective are jurisdictions at preventing money laundering? Insights from the 10th Basel AML Index. Basel AML Index, October 5.

Bellows, A. 2021. An Anti-Corruption Agenda for the Middle Class. Carnegie Endowment for International Peace, July 22.

Bellut, D. 2021. Turkish mafia scandal threatens Erdogan government. Deutsche Welle, May 21.

Biden, J. Carpenter, M. 2018. How to Stand Up to the Kremlin. Foreign Affairs, January/February.

Bjorklund, K. 2021. Trump's Inexplicable Crusade to Help Iran Evade Sanctions. Foreign Policy, January 9.

Burgis, T. 2020. Kleptopia: How Dirty Money is Conquering the World. Harper Collins

C4ADS. 2018. Sandcastles: Tracing Sanctions Evasion Through Dubai's Real Estate Market.

Cadwalladr, C. Jukes,P.. 2018. Revealed: Leave.EU campaign met Russian officials as many as 11 times. The Observer, July 8.

Chase-Lubitz, J. 2018. Council of Europe Body Expels 13 in Azerbaijan Bribe Case. Organised Crime and Corruption Reporting Project, July 4.

Cinar, A. 2017. Testimony of Ali Cinar, president of Turkish heritage organization. House Committee on Foreign Affairs.

Comsure Group 2016. Reputation laundering a new term to the AML vocabulary.

Conn, D. 2021. Saudi takeover of Newcastle leaves human rights to fog on the Tyne. The Guardian, October 8.

Davis, J. 2021. New Technologies but Old Methods in Terrorism Financing. Project craaft, Research Briefing 2.

Doward, J. 2018. Amnesty criticises Manchester City over 'sportswashing'. The Guardian, November 11.

Dowse, A. Bachmann, S. 2019. Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?.

Dunčikaitė, I. Žemgulytė, D. Valladares, J. 2021. Paying for Views: Solving Transparency and Accountability Risks in Online Political Advertising. Transparency International.

Gartenstein-Ross, D. Zelin, A. 2013. Uncharitable Organizations. Foreign Policy, February 25.

Gatehouse, G. 2019. German far-right MP 'could be absolutely controlled by Russia'. BBC, April 5.

Gibson, O. 2015. five years after FIFA's World Cup gift to Qatar that set a timebomb ticking. The Guardian, December 2.

Global Initiative Against Transnational Organized Crime. 2021. Global Organized Crime Index: Turkey.

Global Witness. 2014. The Great Rip Off: Anonymous company owners and the threat to American interests.

Global Witness. 2020. On The House: How anonymous companies are used to launder money in U.S. real estate. Briefing, September 23.

Greentree, T. 2015. America did hybrid warfare too. *War on the Rocks*.

Golkar, S. 2012. Organization of the Oppressed or Organization for Oppressing: Analysing the Role of the Basij Militia of Iran. Politics, Religion & Ideology, 13(4), pp. 455 –471

Government of Canada. 2021. Guidelines on the National Security Review of Investments. March 24.

Gjøll-Trønning,T. Gall, M. 2021. Danish parliament adopts investment screening act on foreign direct investment. Bech-Bruun, M&A and Corporate Matters, June 2.

Hála, M. 2020. A New Invisible Hand: Authoritarian Corrosive Capital and the Repurposing of Democracy. National Endowment for Democracy.

Hall, G. 2021. The UK's new NSI regime: What do you need to know? Norton Rose Fulbright. November 2021.

Harold, S. Beauchamp-Mustafaga, N. Hornung, J. W. 2021. Chinese Disinformation Efforts on Social Media. RAND Corporation.

Harrison, D. 2021. The Men Who Sell Football. Al Jazeera Investigative Unit, August 9.

Harrison, K. and Gyenter, C. 2020. Strategic Corruption. Offshore Initiative, October 8.

Heldevang,M. 2019. Russia allegedly meddled in Bolivia's controversial election. Quartz, November 16.

Hille, P. 2020. FinCEN Files: The art of evading sanctions. Deutsche Welle, September 20.

HM Treasury and Home Office. 2020. National risk assessment of money laundering and terrorist financing 2020.

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

Keatinge, T. Ruehsen, M. Garnier, L. 2021. A Transatlantic Response to Illicit Finance: Starting at Home. Royal United Services Institute, Financial Crime Insights, October 22.

Kergueno, R. Vrushi, J. 2020. Debugging Democracy: Open data for political integrity in Europe. Transparency International.

Klasfeld, A. 2019. Boom Times for Turkey's Lobbyists in Trump's Washington. Courthouse News Service, October 31.

Kurlantzick, J. 2019. How China Is Interfering in Taiwan's Election. Council on Foreign Relation, November 7.

Kux, D. 1985. Soviet Active Measures and Disinformation: Overview and Assessment.

Lafuente, J. Camhaji, E. Gallegos, Z. Zerega, G. Deniz, R. Scharfenberg E. 2021. How a vast network allowed Venezuela to evade US oil sanctions. El Pais, June 16.

Laughland, O. 2017. Fifa officials took bribes to back Qatar's 2022 World Cup bid, court hears. The Guardian, November 15.

Lenihan, A. 2021. Foreign investment regimes: three things the West needs to better protect national security. LSE blogs, March 1.

Levin, S. 2017. Did Russia fake black activism on Facebook to sow division in the US? The Guardian, September 30.

Lobbying Transparency. 2015. International Standards for Lobbying Regulation.

Lynch, I. 2021. The Strategic Cost of Transnational Corruption. The Strategy Bridge, April 12.

Martini, M. 2019. Who is behind the wheel? Fixing the global standards on company ownership. Transparency International.

McGinty, R. 2010. Warlords and the liberal state building in Afghanistan. Conflict, Security and Development 10 (4)

Meester, J. van den Berg, W. Verhoeven H. 2018. Riyal Politik The political economy of Gulf investments in the Horn of Africa. Clingendael Institute.

Moskowitz, E. 2020. Assad's Cousin Says Offshore Companies Helped Evade Sanctions. Organized Crime and Corruption Reporting Project.

Mueller, R. 2019. Report on The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II. US Department of Justice, March 2019.

Murray, M. Vindman, A. Bustillos, D. 2021. Assessing the Threat of Weaponized Corruption. Lawfare, July 7.

New Zealand Department of the Prime Minister and Cabinet. 2017. Defining National Security The agencies' role in protecting New Zealand.

Norell, M. 2020. Erdogan's Influence in Europe: A Swedish Case Study. The Washington Institute, June 4

OECD. 2009. Recommendation of the Council on Guidelines for Recipient Country Investment Policies relating to National Security

Ohman, M. 2020. Note on third party regulations in the OSCE region. OSCE, ODIHR, April 20.

Open Ownership. 2021. The Open Ownership Principles. July 2021.

Ottolenghi, E. Badran T. 2020. Hezbollah Finance in Lebanon: A Primary Source Review. Foundation for Defence of Democracies, September 23.

Parliament of Australia. 2017. Second interim report on the inquiry into the conduct of the 2016 federal elections: foreign donations.

Pevehouse, J. Vabulas, F. 2019. Nudging the Needle: Foreign Lobbies and US Human Rights Ratings. International Studies Quarterly, 63(1), Pp. 85–98,

Pieper, O. 2018. Germany and the long arm of Turkey's AKP. Deutsche Welle, May 18.

Putze, A. 2020. Corruption and Finance in the UK. Royal United Services Institute, Financial Crime Insights, November 12 [podcast].

Rahman, K. 2021. Supervisory and professional bodies dealing with professional enablers of IFFs. U4 Helpdesk Answer.

Remeur, C. 2019. Understanding money laundering through real estate transactions. European Parliament Research Service.

Reuters. 2017. Qatar-linked People, Groups on Terror List, Reuters, 9 June 2017

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

Ross, A. 2019. Opacity: Why Criminals Love Canadian Real Estate (And How to Fix It). Transparency International Canada.

RTE. 2015. FIFA executive Committee 2010: Where are they now? December 1.

Rudolph, J. 2021. The Five Great Enabler Nations. Alliance for Securing Democracy, November 9.

Rudolph, J. Morley, T. 2020. Covert Foreign Money. The Alliance for Securing Democracy. August 18.

Schmeidl, S. 2016. The contradictions of democracy in Afghanistan: elites, elections and 'people's rule' post-2001, Conflict, Security & Development, 16(6), pp. 575-594.

Schneider-Petsinger. 2016. Geoeconomics explained. Chatham House, December 9.

Seely, B. 2021. Foreign Interference Unchecked: Models for a U.K. Foreign Lobbying Act. The Henry Jackson Society.

Seldin, J. 2021. US: Russia, Iran Meddled in November's Election; China Held Back. Voice of America, March 16.

the Sentry. 2021. Artful Dodgers: New Findings on North Korean Sanctions-Busting in the Democratic Republic of the Congo. January 2021

Skoumal, T. Malkovsky, M. Simcina, M. 2021. Slovakia introduces new foreign investment screening scheme. Foreign investment and security blog, April 13.

Solomon, M. 2019. Illicit Financial Flows to and from 148 developing countries: 2006-2016. Global Financial Integrity.

Sonne, P. 2018. A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening. Washington Post, December 27.

Spicer, J. 2021. Finance watchdog 'grey lists' Turkey in threat to investment. Reuters, October 21.

Splidsboel, F. 2017. Russian Hybrid Warfare: A study of disinformation. Danish Institute for International Studies, August 22.

Strøm, O. 2021. Økokrim-sjefen: - Norge bør boikotte Qatar-VM. Aftenposten, October 28. [In Norwegian]

Sutton, T. Clark, S. 2020. How Biden Can Defeat Strategic Corruption. Just Security, December 17.

Švedkauskas, Ž. Sirikupt, C, Salzer, M, 2020. Russia's disinformation campaigns are targeting African Americans, Washington Post, July 24.

Talley, I. 2019. U.S. Targets 'Vast Network' Evading Iran Sanctions. The Wall Street Journal, March 26.

Transparency International UK. 2018. In whose interest? Analysing how corrupt and repressive regimes seek influence and legitimacy through engagement with UK Parliamentarians Transparency International UK, July 2018.

Transparency International UK. 2019. At Your Service: Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations.

Transparency International. 2021. What the global standard on company ownership should look like: Five key areas. August 6.

UNODC. 2020. Conceptual Framework for the Statistical Measurement of Illicit Financial Flows.

US Congress. 2021. ENABLERS Act.

US Treasury. 2018. Treasury Designates Russian Oligarchs, Officials and Entities in Response to Worldwide Malign Activity. April 6.

Valladares, J.V.M. n.d President of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation.

Vidino, L. 2019. Erdogan's Long Arm in Europe. Foreign Policy, May 7.

Vittori, J. 2021. Five Things the United States can Do to Stop Being a Haven for Dirty Money. Carnegie Endowment for International Peace, October 7.

Walker, C. 2018. What is "Sharp Power"? Journal of Democracy 29 (3), pp. 9-23.

Weinthal, B. 2021. Qatar has send hundreds of millions of dollars to terror group – report. The Jerusalem Post, June 6.

White House. 2021. Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest, June 3.

White, M. 2017. I started Occupy Wall Street. Russia tried to co-opt me. The Guardian, November 2.

Winter, C. 2017. Turkish AKP politician linked to Osmannen Germania boxing gang in Germany. Deutsche Welle, December 14.

Zelikow, P. Edelman, E. Harrison, K. Gventer C. 2020. The rise of strategic corruption: how states weaponise graft. Foreign Affairs, July/August 2020.

**DISCLAIMER**

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

**PARTNER AGENCIES**

GIZ/BMZ (Germany), Global Affairs Canada, Ministry for Foreign Affairs of Finland, Danida (Denmark), Sida (Sweden), SDC (Switzerland), Norad (Norway), FCDO (UK).

**ABOUT U4**

The U4 anti-corruption helpdesk is a free research service exclusively for staff from U4 partner agencies. This service is a collaboration between U4 and Transparency International (TI) in Berlin, Germany. Researchers at TI run the helpdesk.

The U4 Anti-Corruption Resource Centre shares research and evidence to help international development actors get sustainable results. The centre is part of Chr. Michelsen Institute (CMI) in Bergen, Norway – a research institute on global development and human rights.

www.U4.no
U4@cmi.no

**KEYWORDS**

Strategic corruption – illicit financial flows – political interference