Open Ownership

Using beneficial ownership data for **national security**

December 2021

Contents

Overview

National security is a broad concept which has evolved as the ability of a state to protect and defend its citizens to include its society's norms, rules, institutions, and values more broadly.[1, a] There has been an increasing focus on how anonymously owned companies can create a threat to national security, and therefore how transparency and visibility of the individuals who ultimately own and control companies – the beneficial owners – can help protect it. There is a range of ways in which a lack of visibility on company ownership can help malign actors circumvent domestic legislation and create loopholes that present security threats, ranging from physical security threats to citizens (e.g. crime and terrorism) to interference with governance (e.g. political corruption, and undermining democracy and the rule of law).

In December 2020, the United States (US) committed to the implementation of a central – albeit non-public – beneficial ownership (BO) register. The main stated reason for the US commitment has been to protect national security.[2] In June 2021, President Biden published a memorandum in which he listed the reporting of beneficial owners and the reduction of offshore financial secrecy as solutions to "countering corruption as a core United States national security interest."[3] The idea that anonymously owned companies can present security threats has also gained attention through the focus on the influence of foreign funding on domestic politics, such as in Australia[4] and in the European Union (EU).[5] Despite the rhetoric of beneficial ownership transparency (BOT) in the national security context, there is little detailed examination of its role.

Over a hundred jurisdictions have committed to the implementation of BOT reforms, which aim to make information about beneficial owners available to a range of actors who use the data to achieve certain policy goals.[6] BOT, and the use of BO data more broadly, can be used to further numerous policy aims. As the use of BO data emerged in anti-money laundering (AML), its roots are, arguably, in the field of national security.

The US and other countries started implementing AML policies in earnest from the 1970s in response to the drug trade, at a time when the Soviet Union actively encouraged narcotics trafficking by its non-state proxies.[7] The body of AML policies expanded to incorporate countering the financing of terrorism (CFT) during the 1990s, and CFT policies were widely adopted following the 11 September 2001 terrorist attacks.[8] More recently, BOT has proven useful in a range of other policy areas, including: domestic resource mobilisation (e.g. by preventing tax evasion and in assessing the feasibility and enforcement of a wealth tax[9]); public procurement;[10] improving the ease of doing business (e.g. by helping companies better manage risk and leveling the playing field);[11] and resource governance (e.g. in the extractives industry).[12] A comprehensive review of how these policy areas may intersect with the subject of national security and how BOT, specifically, can further national security policy aims has not been conducted.

This briefing sets out how BOT can contribute to specific national security aims across different policy areas. It will focus specifically on the nation state, and on how the implementation of BOT domestically can help further national security aims. The activities of a foreign state or actor in a third country, the perceived threats they may pose, and the ways in which the implementation of BOT in third countries can mitigate these threats are outside the scope of this briefing. In other words, the briefing will not consider potential national security threats to Country A caused by Country B's activities in Country C, for a few reasons. First, these perceived threats might be more geopolitical in

a For example, New Zealand includes protecting the country's "status as a free and democratic society from unlawful acts or foreign interference" in its national security definition. At China's National Security Commission's first meeting on 15 April 2014, President Xi Jinping articulated the concept of 'holistic' or 'overall national security' (*Zongti guojia anquanguan*), comprising 11 areas of concern, including political security, which has also been institutional security or ideological security. See: "Defining National Security: The agencies' role in protecting New Zealand", Department of the Prime Minister and Cabinet, September 2017, https://dpmc.govt.nz/sites/default/files/2017-09/fact-sheet-3-defining-national-security_1.pdf; Shen Dingli, "Framing China's National Security", *China US Focus* (blog), 23 April 2014, https://www.chinausfocus.com/peace-security/framing-chinas-national-security/.

nature and difficult to substantiate, delineate, and define. Second, BOT is most often implemented through a series of reforms at the national level (i.e. Country A does not regulate company ownership transparency in Country C), so is beyond the scope of their action. Third, Country C might welcome Country B's activities, as can be argued, for instance, in many countries involved in the Belt and Road Initiative.[b]

The briefing will illustrate key BOT use cases for national security using country examples from across the globe. Due to the US focus on this issue, many of the case studies in this briefing will look at the US. The briefing concludes that BOT can help mitigate a range of national security threats, and focuses on five areas. It will start with the policy areas where BOT has its roots. These subjects are already well covered, but the specific added value of BO data in the context of national security is less so:

- preventing **corruption and organised crime**;
- countering the financing of **terrorism**;
- enforcing **economic and financial sanctions** on individuals, organisations, and jurisdictions.

Subsequently, the briefing will look at more recent national security use cases of BOT:

- protecting **strategic sectors**;
- preventing interference in **governance systems** and the **rule of law**.

These issues can have both a direct and indirect bearing on national security. The policy areas are interlinked, but the nature of the security threats, and the ways in which anonymous companies exploit loopholes that BOT can help close, are different. In certain cases, companies can be used to effectively make a country complicit in illegal activities outside its jurisdiction, which can negatively impact national security. In other cases, companies are used to circumvent domestic laws which are in place to safeguard national security interests (e.g. political lobbying regulations). A number of these relate to corruption, whilst others relate to fraud or the enforceability of established legislation. In all cases, corporate structures are used to hide the true identity of those who actually own and control companies.

The threats can involve both state and non-state actors. It is often difficult to determine whether activities that pose potential security threats emanate from state or non-state actors, and where the difference is unclear (e.g. with state-owned or state-linked companies, or with state-owned or politically linked companies). Anonymous companies can be used by both state and non-state actors as an intentional tactic to exploit security weaknesses in a country. Other times the intent can be different (e.g. self-enrichment), but the action can nevertheless be damaging to national security. The term *strategic corruption* describes cases where actions are coordinated by a hostile state and there is clear intent to undermine national security.[c] The actions themselves may involve non-state actors, with or without their knowledge. The use of anonymously owned corporate structures makes it very hard to know if a state actor is involved. In strategic corruption, corrupt inducements are wielded against a target country by foreigners as a part of their own country's national strategy.[13]

National security cuts across a range of policy areas, and, therefore, BO information will need to be made available to a range of different actors to effectively counter security threats. BOT and the presence of BO data alone will not achieve policy outcomes. Impact requires the data to be usable and used, and may need complementary legislation which the data can help monitor and enforce. The main value of BO data is its use in combination with other relevant data (e.g. procurement data), meaning structured and interoperable data is most effective. Foreign state ownership of companies is relevant and should therefore be captured as part of BO disclosures in a standardised way.[14] To achieve its aim, central and public BO registers provide the most effective access to the broadest range of different actors.[d] Beyond specific use cases, BOT provides visibility and knowledge of who is operating in an economy and financial system, which is fundamental information for knowing how best to protect it.

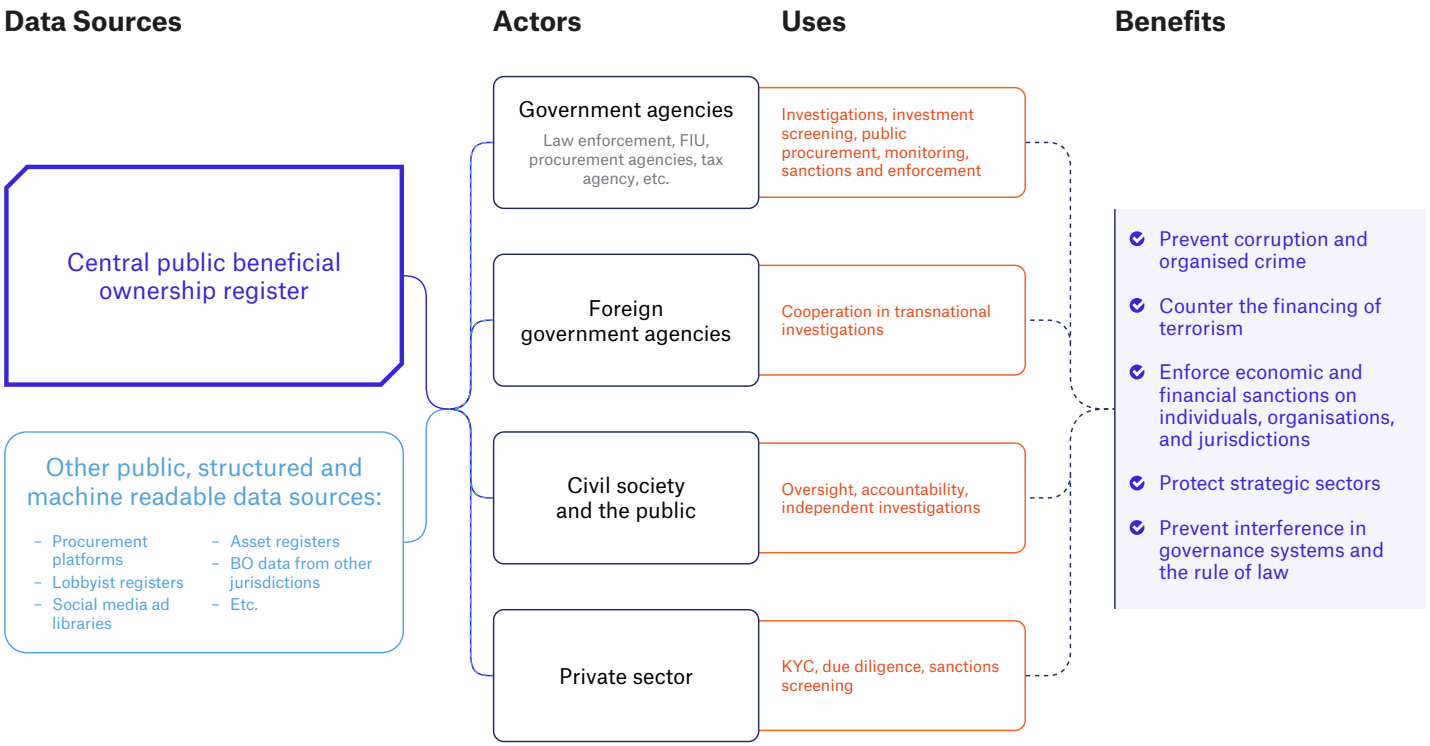
---

b The Belt and Road Initiative is a major Chinese global infrastructure development strategy, adopted in 2013, that seeks to connect Asia with Africa and Europe via land and maritime networks through significant infrastructure investments. Around 140 countries have signed up to the initiative. It is considered part of China's growing efforts to exert influence which is seen by some other countries as a threat. See: Wendy Leutert and Jack Nolan, "Signing up or standing aside: Disaggregating participation in China's Belt and Road Initiative", Brookings, October 2020, https://www.brookings.edu/articles/signing-up-or-standing-aside-disaggregating-participation-in-chinas-belt-and-road-initiative/.

c Also known as *weaponised corruption*.

d Kiepe, "Making central beneficial ownership registers public". These and other best practices for effective beneficial ownership disclosure are detailed in the Open Ownership Principles. Effective disclosure generates actionable and usable data across the widest range of policy applications, and minimises loopholes. See: "Principles for Effective Beneficial Ownership Disclosure", OO, July 2021, https://www.openownership.org/principles/.

Figure 1. How beneficial ownership information can be used for national security



The diagram visualises the flow of BO information and complementary data to actors that can contribute to safeguarding national security. Governments can collect and verify BO information in central registers for all companies in an economy as part of commitments or international obligations. Central registers are the most effective way to provide access for authorities. Making the information public means the data is available to the widest possible set of actors, and can decrease access times for certain data users, such as foreign law enforcement. Structured data is more easily integrated with other data sources and improves overall usability.

BO information can be used by actors in a range of different ways to strengthen a range of national security outcomes, including by using data in investigations and due diligence, monitoring, sanctioning and enforcing legislation, and to screen investments and improve public procurement. This helps prevent corruption and organised crime (page 6); counter the financing of terrorism (page 8); enforce economic and financial sanctions on individuals, organisations, and jurisdictions (page 10); protect strategic sectors (page 13); and prevent interference in governance systems and the rule of law (page 17).

Preventing corruption and organised crime

Both domestic and foreign corruption, as well as organised crime, can form national security threats. Domestic corruption has long been recognised as a potential threat to peace, stability, and security (for instance, by compromising human rights and eroding trust in government).[15] More recently, the focus has shifted to how corruption in one country can have national security implications for another. Whilst academics question the causality between corruption and conflict,[16] the co-occurence of corruption along with other drivers, where and when global security threats emerge, has been well documented.[17] Corruption has also been linked to transnational organised crime. Corruption can enable some economic crimes, and they share similar drivers and rely on similar mechanisms to move and launder illicit funds.[18] Transnational crime was declared a national security threat by the US Obama administration, stating that it had "dire implications for public safety, public health, democratic institutions, and economic stability".[19] A 2020 national risk assessment in the United Kingdom (UK) said organised crime has "more impact on UK citizens than any other national security threat" by affecting public services, infrastructure, and vulnerable individuals.[20]

Even if the act of corruption or crime occurs in another country, domestic policies are relevant because those who profit from corruption or transnational crimes often move the illicit proceeds abroad through the globalised financial system. Foreign actors can use domestic institutions to hide, safeguard, invest, and spend the proceeds. Often they are attracted to and use Western financial institutions, due to the openness of their economies and the veneer of legitimacy they provide.[21] As research and multiple leaks and investigations have shown, major Western financial centres are a key conduit for the proceeds of corruption and transnational crime.[22] For instance, the 2020 UK National Risk Assessment of Money Laundering and Terrorist Financing estimated money laundering in the UK to potentially be in the hundreds of billions of pounds annually, saying that the majority of this is likely to be corrupt money from outside the UK.[23] Complex corporate structures are often set up in jurisdictions that do not have transparency requirements for company ownership. Such arrangements allow funds to enter the financial system; create distance between the perpetrators and their proceeds; and enable wealth to be acquired from the proceeds, often by integrating the funds into the formal financial system.

Countries have been trying to fight corruption both at home and abroad through extraterritorial anti-bribery legislation that criminalises paying, receiving, and handling the proceeds of corruption.[24] Corruption is also increasingly being recognised as a predicate crime for money laundering offences. AML policies seek to tackle corruption and other crimes, such as narcotics trafficking indirectly by targeting their profits. The EU's proposed sixth Anti-Money Laundering Directive (AMLD6), for instance, defines and standardises 22 predicate offences for money laundering in all EU member states, including corruption.[25] Such policies place corruption squarely within the scope of AML legislation, the international standards of which are set by the Financial Active Task Force (FATF), the inter-governmental policy body founded in 1989 by the G7.[26] Part of the FATF Standard are recommendations for preventive measures to stop criminals from using financial institutions and certain designated non-financial businesses.

AML legislation places requirements on so-called obliged entities to carry out due diligence on clients as part of know-your-customer (KYC) requirements, and report suspicious activities and transactions to financial investigative units (FIUs). These entities are most commonly financial institutions, but in some jurisdictions also include the insurance, real estate, law, and accounting sectors – also known as designated non-financial businesses and professions (DNFBPs).

Box 1: The United States: crime, corruption, and national security

On 25 July 2011, the Obama administration released the Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security. In it, the government states that the penetration of transnational organised crime into government and institutions is "exacerbating corruption and undermining governance, rule of law, judicial systems, free press, democratic institution-building, and transparency".[27]

In June 2021, US President Biden's administration went further, stating that corruption "contributes to national fragility, extremism, and migration; and provides authoritarian leaders a means to undermine democracies worldwide".

"Corruption threatens United States national security [...] and democracy itself. But by effectively preventing and countering corruption and demonstrating the advantages of transparent and accountable governance, we can secure a critical advantage for the United States and other democracies."[28]

The role of beneficial ownership transparency

BO as a concept, and BO information as a resource, emerged as part of the customer due diligence and KYC obligations established under AML regulations, to identify the real individuals behind companies. In order to address challenges around data quality and speed of access for law enforcement, G8 countries agreed in 2013 to a set of principles for companies to make their BO information available to law enforcement and other competent authorities, a requirement that was reiterated by FATF in 2014. In the next few years, a number of countries, starting with Ukraine and the UK in 2015 and 2016, implemented BOT by establishing central registers and collecting, verifying, and publishing BO data. Since then, central registers have emerged as the most effective way of making BO data available to competent authorities fighting financial crime. Making this data public furthers AML aims by making the data available to a wider set of actors fighting financial crime, such as civil society and investigative journalists.

Whilst critics have been skeptical about the effectiveness of broader AML legislation,[29] conversations with law enforcement testify to the value of BO data in criminal investigations. BO disclosures can be useful in these investigations regardless of whether the information in them is a representation of the truth, as the information contains claims about ownership at particular points in time, which can be compared to other records. The information can help identify individuals with some level of real responsibility in a company and help identify links between companies to each other through individuals.[30] Central and public registers are core tenets of an effective disclosure regime.[31]

BO data can also be used to fight corruption domestically by using it in procurement processes. As procurement corruption presents a different set of national security threats, this will be discussed in more detail further on.

Countering the financing of terrorism

The Global Terrorism Database and the Global Terrorism Index define terrorism as "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation". Following this definition, jurisdictions on all continents are affected by terrorism, and it is subsequently deemed a national security threat in most jurisdictions.

Following the 11 September 2001 terrorist attacks, the US government and North Atlantic Treaty Organization (NATO) allies focused their attention on terrorist financing.[32] A United Nations (UN) Security Council resolution supported the endeavour,[e] and the FATF extended its remit and issued eight (later nine) Special Recommendations on Terrorism Financing in October 2001. Since then, countering the financing of terrorism (CFT) has gone hand in hand with AML, frequently jointly referred to AML/CFT.

There has been both criticism and support for placing a responsibility with companies to counter the financing of terrorism. Critics argue that it is one thing for the government to give financial institutions a list of names of people it deems terrorists,[f] but that it is unrealistic for financial institutions to detect suspected financing of terrorism if the government itself does not fully understand how terrorism is financed.[g] The idea that anonymously owned shell companies[h] are widely used in terrorism financing is one that has entered public discourse but not one for which much publicly available evidence exists, especially for more recent international terrorism threats. The EU's fifth Anti-Money Laundering Directive (AMLD5) was deemed a response to the 2015 terror attacks in France and Belgium, despite the main method of moving and using funds being prepaid cards rather than legal entities.[33] The attacks are thought to have been largely self-funded through job earnings and government benefits.[34]

A review of 263 cases in the US found only "one instance where a shell company might possibly have been involved, nine instances where active charities were involved, and six instances where legitimate companies were involved". Another part of the same research project focused on non-US cases and found no instances involving shell companies.[35] Whilst it is believed significant financial infrastructure is required to sustain international terrorist networks,[36] the sums involved in terrorist attacks and transfers abroad to sustain these networks are small. In many cases, the source is not necessarily illicit and often largely cash-based.[37] Consequently, the search by banks for transactions potentially funding terror is challenging, and has limited success.[38] This leads some to conclude the war on terrorism financing has failed.[39] Meanwhile, the response by financial institutions has been to de-risk or fully end business relationships with certain clients or categories of clients (e.g. based on geography) due to the challenges in assessing risk. This can have the counterproductive consequence of pushing financial flows into less regulated (e.g. cash-based) channels, and can sever remittance channels.[40]

There is also evidence that, despite global uptake of regulations, enforcement actions against state-affiliated financial institutions can fail, especially when this conflicts with local national security priorities.[41] Others say the war on terrorism financing has been more successful than other

---

e See: S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001): Recognising "the need for States to complement international cooperation by taking additional measures to prevent and suppress ... the financing and preparation of any acts of terrorism".

f International sanctions lists, such as the US one administered by the Office of Foreign Assets Control (OFAC), contain individuals suspected of a range of crimes, including terrorism.

g The 9/11 Commission extensively reviewed the financing of the 9/11 attacks and found no apparent terrorism financing indicators. See: Richard Gordon, "A Tale of Two Studies: The Real Story of Terrorism Finance", *University of Pennsylvania Law Review* 162 no. 269, 2014, 274, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1129&context=penn_law_review_online.

h A shell company is a company that engages in no substantive business activities, but instead exists as a vehicle, typically to make use of a particular legislation in another country, shield another party from liability, or hide a company's true owner.

efforts to fight terrorism, if measured by the global adoption of CFT legislation.[42] There are several cases where there has been evidence of designated terrorist groups using shell companies where the line between terrorism and organised crime blurs. For example, the Revolutionary Armed Forces of Colombia (FARC), which Colombia and others designated a terrorist organisation in 1997, was heavily involved in organised criminal activities, including drug-trafficking, to finance its activities and had an extensive transnational money laundering network.[43]

The role of beneficial ownership transparency

BOT is most relevant for national security where corporate entities are involved, and where there is a crossover between organised criminal activities and terrorist networks. Whilst there is less evidence of anonymously owned shell companies being used in terrorism financing than the policy response may suggest, it is possible for these structures to be used for financing terror. BO disclosures can play a crucial role in preventing this from happening and deterring abuse of corporate structures for these purposes. However, for this to be effective, governments should make up-to-date lists of known and suspected terrorists and financiers available to financial institutions and DNFBPs, and successfully enforce transgressions.[44] This will be further explored in the following section on economic and financial sanctions. Full transparency in company ownership allows all companies to know with whom they are doing business, and would therefore make it easier for them to screen the names of individuals behind companies. BOT could serve as a deterrent to anonymously owned companies being abused by a range of actors, including terrorism financiers. However, BOT is by no means a silver bullet for countries aiming to tackle terrorism financing, as many of the financial channels used will remain out of scope of these measures.

Enforcing economic and financial sanctions

Sanctions are part of diplomatic efforts to protect national security interests and international law, and defend against threats to international peace and security. There are different types of sanctions, but the main type that is relevant to BOT is economic and financial sanctions, which can be imposed on nations, organisations, or individuals, and are often associated with organised crime, terrorism, hostile states, or proliferation financing.[i] The use of sanctions can involve seizing or freezing assets, and banning trade and financial transactions with the target of the sanctions. Violating sanctions is often a criminal offence. There are international sanctions lists, such as the United Nations Security Council Consolidated List, the World Bank Ineligible Firms and Individuals List, the Interpol Wanted List, and the EU Consolidated List. Additionally, many countries maintain their own sanctions list, for example, the US Office of Foreign Assets Control (OFAC) Specially Designated Nationals List and the UK HM Treasury Financial Sanctions List. National sanctions lists are a predominantly Western phenomenon, but other countries, such as China, also have sanctions lists.[45]

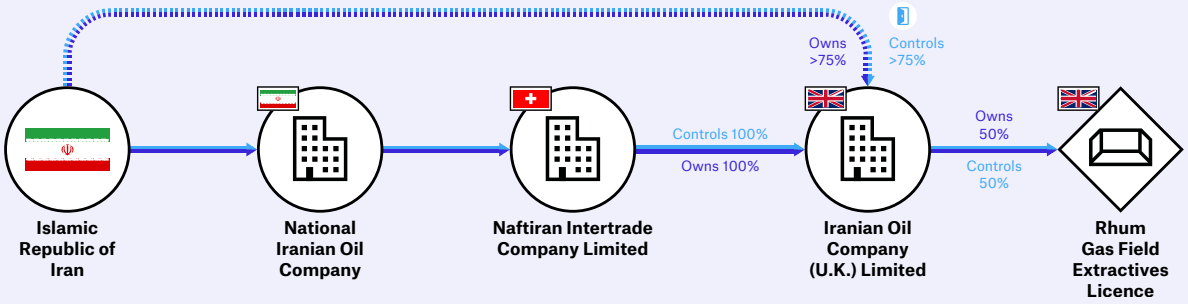
Checking against sanctions lists is a common part of onboarding new customers and ongoing due diligence by regulated entities under AML/CFT regulations. Nevertheless, anonymously owned shell companies – including entities in the sanctioning jurisdiction – can be, and are frequently, used to evade sanctions (see, for example, Box 3 and Box 4). Arguably, these cases could be prevented if better information about the ownership of companies was widely available.

---

i Proliferation financing comprises financial products and services which are directly linked to the trade in proliferation-sensitive items, such as chemical, biological, radiological, and nuclear weapons. See: "National risk assessment of proliferation financing", 13.

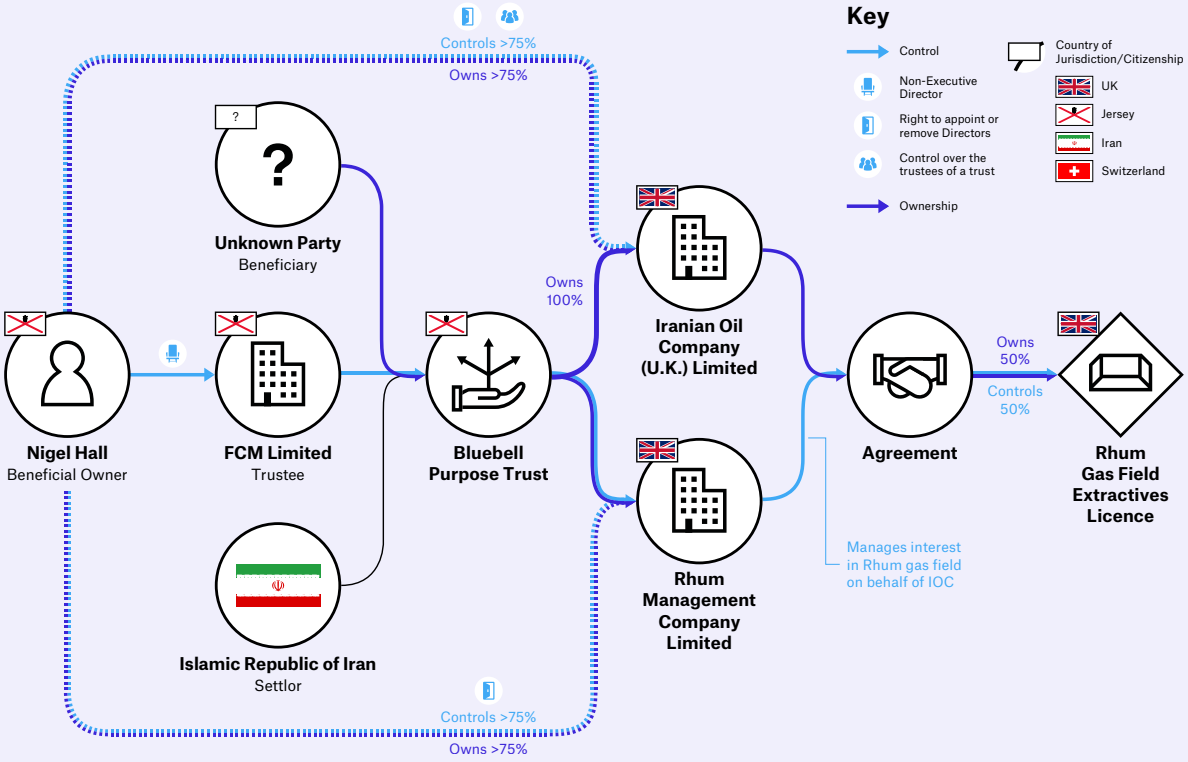
Box 2: Iranian Oil Company (U.K.) Limited and the UK BO register

Figure 2. Ownership and control structure of Iranian Oil Company (U.K.) Limited before 2 November 2018



Iranian Oil Company (U.K.) Limited (IOC) is an oil and gas company that holds a licence in the UK for a 50% interest in the Rhum gas field in the North Sea.[46] Following new US sanctions against Iran in 2018, OFAC required the Iranian government's shareholding to be transferred into a trust so that Iran could not derive any benefit or exercise any control from the Rhum gas field while the US sanctions are in place.[47]

Figure 3. Ownership and control structure of Iranian Oil Company (U.K.) Limited after 2 November 2018



Sources: UK Companies House and US Securities and Exchange Commission.

On 2 November 2018, the UK's BO register showed the cessation of the Islamic Republic of Iran as the beneficial owner of IOC, along with the termination of three Iranian directors. On the same date, the register shows Jersey-registered FCM Limited incorrectly listed as the new beneficial owner.[j, 48] Filed annual accounts show that, with effect from 2 November 2018, all of IOC's shares were transferred to the Bluebell Purpose Trust, with FCM Limited as corporate trustee.[49] From December 2020, the UK register lists the non-executive chair of FCM Limited as the beneficial owner. That same person is also the beneficial owner of a management company set up to manage IOC's interest in the gas field.[50] This example shows how BO and company data can be used to monitor and enforce sanctions. It also shows the challenges opaque structures such as trusts pose in ensuring sanctions compliance, as the conditions of the trust are unknown.

j According to both international standards and the UK definition of BO, a beneficial owner must be a natural person, and cannot be a legal entity.

Box 3: Evasion of US sanctions against Iran through shell companies

The US has had sanctions in place against the Islamic Republic of Iran – which it deems a threat to its national security – since 1979. In March 2021, charges against 10 Iranian nationals included the use of shell companies to disguise transactions to evade American sanctions against Iran. The individuals are charged with disguising more than USD 300 million worth of transactions over the course of nearly 20 years – including the purchase of two USD 25 million oil tankers – on Iran's behalf through front companies in a number of jurisdictions, including in the US itself. As part of the scheme, "the defendants allegedly created and used more than 70 front companies, money service businesses and exchange houses". In 2016, one of the accused allegedly transferred USD 66,766 into the US on Iran's behalf via a Santa Monica-based company with a bank account held at Wells Fargo & Co.[51]

The role of beneficial ownership transparency

BO information can be critical for successful investigations into sanctions violations. Research shows that networks set up to evade US sanctions against North Korea use several layers of entities to obscure connections to the sanctioned country, which reduces "the scrutiny of their financial transactions in the international financial system [...] North Korean front and shell companies often share patterns such as co-locating business addresses and beneficial owners", as was the case for multiple implicated UK companies.[52] Bulk analysis of BO information can facilitate the identification of companies sharing beneficial owners and addresses, which can aid (proactive) investigations into the violations and evasion of sanctions. In addition to financial flows, economic and financial sanctions often also cover non-financial assets. BO data can also be used by different government agencies in their due diligence processes to prevent sanctions evasion through the specific assets they issue licences for, for instance aircraft (see Box 4) or vessels.[53] Given the range of government agencies potentially involved, governments are recommended to collect and verify the information centrally. It is also critical for BO disclosure regimes to capture sufficient detail about state ownership, as recommended by the Open Ownership Principles (OO Principles),[54] as state involvement may not be immediately obvious.[55]

Box 4: Evading US sanctions through aircraft ownership

A 2020 study by the US Government Accountability Office (GAO) found that the government body that registers civilian aircrafts, the Federal Aviation Administration (FAA), "generally relies on self-certification of registrants' eligibility and does not verify key information".[56] It concluded that the system is "vulnerable to fraud and abuse when applicants register aircraft using opaque ownership structures that afford limited transparency into who is the actual beneficial owner". The body that manages the US sanctions list, OFAC, can freeze assets, including aircraft, under US jurisdiction.

In a case study, the GAO details how, in 2017, the OFAC sanctioned the Executive Vice President of Venezuela for his role in international drug trafficking. According to the OFAC, the Venezuelan government official facilitated drug shipments to Mexico and the US, by using a frontman to launder proceeds and purchase assets. According to the OFAC, in addition to a network of international companies, this frontman owned or controlled five US companies. One of these companies, a limited liability company (LLC), registered an aircraft with the FAA using a trust to meet US citizenship requirements for aircraft ownership. Unrelated to the designation, the FAA deregistered the aircraft. The FAA subsequently issued a dealer certificate to the LLC after the sanctions designation, as it was unaware the designation had been made.[57]

Specifically, a challenge for the FAA is that the ownership data on individuals and entities "are stored in files that cannot be readily analyzed due to system limitations".[58] Making centrally collected and verified BO information available as structured, machine-readable data could help facilitate automated red-flag checks for aircraft ownership. Besides sanctions evasion, aircraft ownership by the wrong individuals can also pose a more direct physical safety concern.

Protecting strategic and sensitive sectors

Threats to strategic and sensitive sectors, such as defence, energy, telecommunications, or sectors producing dual-use items,[k] emerge through the inadvertent or intentional acquisition of ownership by hostile actors. These can also be caused by weaknesses in public procurement, such as corruption or the lack of due diligence. BO data can address both these threats by aiding investment screening and improving public procurement.

Investment screening

A number of countries have policies in place to prevent the acquisition of ownership in strategic and sensitive sectors, or more broadly for any foreign direct investment, by actors with links to hostile foreign states. Broadly, these policies put in place (foreign) investment screening mechanisms. The COVID-19 crisis has seen an increase in these policies to prevent opportunistic takeovers and acquisitions in a time when many companies find themselves in financial trouble.[59] Governments often impose investment restrictions on specific strategic sectors. For instance, the Dutch parliament is currently discussing the "Investments, Mergers and Acquisitions Security Screening Bill" which identifies "vital suppliers" (heat transport, nuclear power, air transport, ports, and banking services) and "sensitive technologies" (including military goods) to be brought within the scope of the legislation due to their relevance for national security.[60] The bill will require detailed information regarding "the identity of the investors and ultimate beneficial owners, the control structure and value of the investment, the origin of financial resources, the business activities of the investor and the target, and criminal records".[61] A UK act commencing in January 2022 defines 17 sensitive sectors, ranging from synthetic biology to dual-use goods, which are subject to screening for investment and intellectual property, and export controls.[62] The application of the law is defined by thresholds of ownership and control.[63]

Many countries also have regulations governing media ownership, typically to ensure public opinion and policies are not influenced unduly and to encourage media pluralism. In September 2021, Ukraine adopted an "anti-oligarch" bill aimed at curbing the political influence of powerful individuals associated with corruption in the country, which implements a register of individuals who qualify as an oligarch by meeting a number of criteria, including significant influence over the media.[64] In Armenia, a central public register for all legal entities is expected to be launched in 2022. Civil society organisations expect that transparency in company ownership will help counter fake news and misinformation, out of concern over political influence being exerted over their media, especially by those with links to Russia.[l] In the Philippines, highly protectionist legislation requires companies that engage in broadcasting to be wholly Filipino-owned,[65] although critics say this lacks enforcement.[66] However, there is a broader debate about the transparency of media ownership and its relation to democracy and the rule of law. The policies discussed may also be used by governments in ways that are not necessarily beneficial to the functioning of democratic governance, for instance, by restricting freedom of speech and control of the media.

---

k Dual-use items are goods, software, technology, documents, and diagrams which can be used for both civil and military applications. See: "National risk assessment of proliferation financing", 9.

l Some media companies are wary this will threaten the freedom of the press. See: Shushan Doydoyan, "Beneficial ownership progress in Armenia", Freedom of Information Center of Armenia, 6 April 2021, http://www.foi.am/en/news/item/2011/.

Box 5: Indian restrictions on foreign direct investment

In response to the COVID-19 crisis, the Indian Ministry of Commerce amended its Foreign Direct Investment Policy in April 2020.

Prior to the amendments, the foreign direct investment laws in India restricted people with Bangladeshi or Pakistani citizenship and entities incorporated in Bangladesh or Pakistan from investing in an Indian company without prior government approval. Further, any citizen of Pakistan or entity incorporated in Pakistan was not permitted to invest in defence, space, atomic energy, and sectors or activities prohibited for foreign investment at all.

The amendments expand the scope of these restrictions to entities from countries sharing a land border with India, and to beneficial owners of investments into India who are resident in or citizens of these countries. Where a transfer of ownership directly or indirectly results in the BO falling within the above restriction, the change in BO also requires prior government approval. Consequently, investments from countries like Afghanistan, Bhutan, China, Myanmar, and Nepal, in addition to Bangladesh and Pakistan, are now also subject to prior government approval.[67]

The role of beneficial ownership transparency

BOT can help make the true owners of companies visible and can ensure that hostile states do not circumvent ownership requirements using domestic shell companies. At a minimum, BO information should be made available to the government bodies that need to enforce investment screening policies. Collecting and holding information as structured data will make access by different bodies easier. Making data available to the public allows for public oversight of government activities; it can increase trust and accountability and provide a range of other potential benefits,[68] for instance, in the case of media ownership. As with public procurement, given the range of policy applications of BO data, governments are recommended to collect and verify the information centrally. It is also critical for BO disclosure regimes to capture sufficient detail about state ownership, as recommended by the OO Principles.[69]

Improving public procurement

Public procurement is the purchase of goods, work, or services by governments. Typically, governments have procurement policies that aim to prevent corruption and fraud as well as foster fair, equitable competition and transparency to deliver value-for-money services for taxpayers through tenders. Governments often attach criteria to supplier eligibility relating to ownership in procurement for strategic sectors, such as defence and security. Governments limit the supply of defence procurement to domestic companies, so that suppliers fall within the government's jurisdiction. Weaknesses in procurement, such as corruption or poor due diligence, can lead to non-delivery, or delivery of faulty or inferior critical goods and services (see Box 7). It can also compromise security by providing confidential information about or control of critical assets to hostile actors (see Box 7 and Box 8). Foreign companies can pose particular due diligence and verification issues, and can bring added risks, such as political officials using offshore companies to hide their interests in a company to access public contracts that they otherwise should not.

Fraud and corruption severely undermine procurement processes. Corruption in procurement involves the abuse of power of office to steer a contract to a specific bidder without detection. This can involve awarding the contract to a company that should not win according to the set criteria, inflating contract values, or including favourable contractual terms, such as removing repercussions for the failure to deliver. As corruption involves the abuse of power of those involved in the procurement process, there is always a link and a conflict of interest between those involved and the companies that win. The majority of procurement corruption cases involve bribes.[70]

Box 6: Corrupt procurement undermines national security in Nigeria

Research conducted by Transparency International (TI) and Civil Society Legislative Advocacy Centre (CISLAC) shows how defence procurement has provided new and lucrative opportunities for the former military chiefs who allegedly stole as much as USD 15 billion through fraudulent arms procurement deals. This threatens Nigeria's internal security and political stability, and weakens Nigeria's counterterrorism capacity against Boko Haram.[71]

The research shows how shell companies (named briefcase companies in Nigeria) are used to facilitate fraud and corruption in defence procurement. In December 2011, for example, unconfirmed reports surfaced about the Ministry of Defence seeking six Mi-17SH military helicopters to support operations against Boko Haram. The tender was not advertised and instead the eight companies were invited to bid for the multi-billion dollar supply contract.

The bidding companies had generic names such as Asset Management Corp Limited and GNY Management and Consulting, and did not have websites, which are red flags that can signify shell companies. The bids also all seemed to be artificially inflated, potentially indicating collusion and canvassing. Two of the bidding companies were chaired by a close associate of then-President Goodluck Jonathan.[72]

Procurement fraud comprises efforts to subvert the procurement process without the knowledge and complicity of officials. Fraud in procurement can be due to false representation, failure to disclose information, and abuse of position.[73] Multiple bidders can co-conspire to rig a bid as a cartel to inflate prices, suppress bids, or submit fake bids in order to steer the selection towards a specific bid. Procurement systems should raise red flags when fraud is suspected, but fraud can be very difficult, as well as time- and resource-consuming, to detect. Companies can also fail to disclose information that allows procurement agencies to conduct proper due diligence, or submit false information to match the profile of the seller that a buyer is looking for.[74]

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. The objective can be to undermine national security, but could also simply be self-enrichment that compromises national security in the process. National security risks can arise from the procurement of goods such as defence assets (see Box 6 and Box 7) or services, such as the leasing of real estate (see Box 8).

Box 7: Certification challenges in US defence procurement

The US has relied on self-certification in defence procurement but, in doing so, the country has seen both financial and nonfinancial fraud. The Department of Defense's (DoD) vendor vetting programme must carry out investigations into contractor ownership, including BO, without access to a central BO register. In an audit, the GAO concluded that the lack of access to accurate information exposed the DoD to national security risks from contractors with opaque ownership structures, and saw individuals circumvent debarment and eligibility criteria for specific contracts.

The GAO reviewed 32 court cases involving DoD fraud between 2012 and 2018. Four cases involved individuals creating domestic shell companies for foreign manufacturers to bid on contracts specifically designated for domestic companies. One of the companies ultimately supplied the DoD with defective and non-conforming parts that led to the grounding of at least 47 aircraft. Three of the companies shared sensitive military technical drawings and blueprints to foreign countries. In 20 of the 32 cases, the GAO identified ineligible contractors using self-certification to fraudulently win bids set aside for companies with majority ownership by women; US citizens who are economically or socially disadvantaged; or service-disabled veteran-owned businesses. In these cases, they either fraudulently used the names of eligible individuals or the figureheads did not actually hold the level of BO or control of the company required.[75]

In another case, the Pentagon discovered that the company it had procured security cameras from had circumvented domestic production requirements[76] by disguising its illegal importation of Chinese surveillance equipment through the use of shell corporations with anonymous ownership records.[77]

Box 8: Leasing high-security space from foreign owners in the US

A GAO review found that, as of March 2016, the US government has been leasing high-security space from foreign owners in 20 buildings, including 6 Federal Bureau of Investigation (FBI) field offices and 3 Drug Enforcement Administration (DEA) field offices. The spaces are used, among other reasons, for classified operations and to store law enforcement evidence and sensitive data. The companies owning the spaces were based in countries such as Canada, China, Israel, Japan, and South Korea. The GAO was unable to identify ownership information for about one-third of all 1,406 high-security leases, because ownership information was not available for all buildings.[78]

Federal officials interviewed said that the national security risks of leasing foreign-owned real estate include espionage, cyber intrusions, and money laundering. This included potentially "collecting intelligence about the personnel and activities of the facilities when maintaining the property," for instance, "by direct observation or surreptitious placement of devices in sensitive spaces or on the telecommunications infrastructure of the facility".[79]

The role of beneficial ownership transparency

For governments to know to whom they are entrusting the supply of critical goods, services, and sensitive information, it is essential that they be able to identify the people ultimately benefiting from and exercising control over supplying companies, and what their interests might be. Whilst managing a range of risks – including operational and financial – by using different kinds of ownership information in public procurement is not new, governments' use of data collected and published as part of BOT remains relatively unexplored. A growing number of countries, including Bangladesh, Colombia, Egypt, and Moldova, have started implementing BOT solely for public procurement purposes.[80]

Specifically for national security, BOT can help prevent fraud and corruption by signaling potential signs of bid-rigging and conflicts of interest, and verifying supplier eligibility where this is based on ownership. Strengthened procurement processes can also protect national security indirectly by improving the value-for-money of what is procured; this is done by fostering competition and managing risk in order to also expand and diversify the supplier base.[81] Research has demonstrated a range of potential benefits of BOT to procurement processes, especially when information is collected on all companies in an economy and made available to the public.[82] Only collecting BO information on bid winners, as some countries do,[83] will not allow BO data to help raise red flags for bid rigging. If data in a central register is structured and interoperable, red-flagging checks can be automated. Collecting BO information on all companies in an economy and making the information public will also help companies conduct due diligence on each other, which can systemically improve procurement, and allows for public oversight. For defence procurement, publishing details of specific contracts may not be appropriate, but automated checks can be built into procurement processes.[m]

---

m See, for example, the Bluetail prototype: https://bluetail.herokuapp.com/tenders/. Bluetail connects contracting and BO data into a platform for procurement authorities. It displays red flags, such as potential conflicts of interests or collusion (the same beneficial owner appearing in multiple bids). See: Alex Parsons, "Visualising conflicts of interests", mySociety, 31 July 2020, https://www.mysociety.org/2020/07/31/visualising-conflicts-of-interests/.

Preventing interference in governance systems and the rule of law

Strategic corruption has been a key focus of the US commitment to BOT. According to the US National Security Study Memorandum, "authoritarian states 'weaponize corruption' to weaken democracy and the rule of law".[84] Strategic corruption can be defined as "corrupt inducements … wielded against a target country by foreigners as a part of their own country's national strategy. Sometimes, but not always, these schemes entail violations of the law, including by citizens of the target country".[85]

The threat of strategic corruption is difficult to quantify and assess, as it implies intent and coordination by one country to directly or indirectly undermine the national security interests of another country. Intentionality can be especially difficult to discern. The "corrupt inducements" can include all the issues discussed in this briefing, for instance, money laundering, corruption of procurement processes, or unlawfully acquiring ownership in foreign strategic sectors. That these are part of a broader strategy or involve state complicity may be impossible to prove beyond doubt. Nevertheless, different countries identify the following key areas as vulnerable to strategic corruption in their national security strategies, that can subsequently form threats to the integrity of governance systems and the rule of law:[86]

- political campaign financing;
- funding the spread of disinformation, alternative media, and social media campaigns;
- buying of political influence.

Whether or not they are coordinated by a hostile state, these activities directly and indirectly interfere with the democratic process and the functioning of the judiciary.[87]

In many cases, there could be an economic incentive which motivates non-state actors to engage in these activities, which could have national security implications. For instance, someone may have a personal or business interest in achieving a particular policy outcome. Whilst corruption of the policymaking process and conflicts of interest undermine the trust in and functioning of government, this may not be part of coordinated actions from a hostile state. Regardless, this presents a security threat. Other measures (e.g. asset disclosures and parliamentary standards) help counter and detect undue political influence – and BOT can also play a role in these – but they are not the focus of this briefing.

The largest concerns for the US and NATO allies are China and Russia. However, using political financing to achieve certain foreign policy outcomes is not limited to authoritarian states, as suggested by the US National Security Study Memorandum. The US, for example, has funded different groups in Afghanistan on numerous occasions.[88]

Box 9: Russian influence in the EU and the US

In 2020, the UK's Intelligence and Security Committee warned about the risk of political interference by Russia in a report that states that Russia "is using a range of methods to seek to disrupt and exert influence on the UK, including political financing and the spread of disinformation".[89]

The report concludes the government failed to protect the UK from Russian influence, stating that government policy had "offered ideal mechanisms by which illicit finance could be recycled through what has been referred to as the London 'laundromat'". It states that Russian influence has now become "the new normal", and that "there are a lot of Russians with very close links to Putin who are well integrated into the UK business and social scene, and accepted because of their wealth". According to OpenDemocracy, most of this is targeted at Conservative party members.[90] For instance, a major political donor was found to have ties to the Russian government, and concerns were raised about the access the donor had to multiple British Prime Ministers.[91]

Advocates for corporate ownership transparency in the US point to the Russian interference in the 2016 US elections,[92] and see the UK as an example of what happens when "strategic corruption goes unchecked," pointing to the amount of Russian money in the UK financial sector and real estate, which they claim give Russia the confidence to "conduct political assassinations" on UK soil.[93]

A 2018 Senate Foreign Relations Committee minority staff report states that Russia seeks to capture foreign elites through offers of partnership, cash payments, and other financial inducements, and uses state-owned enterprises in strategic sectors, money laundering, and the financing of political campaigns. The report also points to the difficulty to discern intentionality from the Russian state, and that it is unlikely that all activities are directed by the government.[94] This is due to the blurring of lines between private and state activities, and licit and illicit funds.[95]

An investigation by Der Spiegel points to links between Russia and German parliamentarians, documenting how Russian money funds media outlets in Germany and social media campaigns with pro-Russian messages. The investigation points to Russian support for a right-wing party which also takes pro-Russian policy positions.[96]

In July 2021, a UK standards body, the Committee on Standards in Public Life, published a report referencing the Intelligence and Security Committee report, warning about loopholes in the campaign financing laws, which could act as "a route for foreign money to influence UK elections".[97] The committee's chair said digital campaigning has made it "harder to track how much is being spent, on what, where and by whom". The report warns about "unincorporated associations",[98] which are not listed on the UK's company and BO registry, meaning their financial backers can remain anonymous. Conversely, a recent Federal Election Commission (FEC) ruling in the US appears to open the door to foreign financing of US referendum campaigns.[n]

Requiring political donors to be registered and to identify the original source of funds will make it harder for overseas donors to anonymously give through shell companies to political campaigns. The UK has had a central and public BO register since 2016, which shows that BOT and the presence of BO data alone will not achieve policy outcomes. The data must be used, and potentially combined with other data, to achieve impact. This may also require complementary legislation, which the data can help monitor and enforce.

The role of beneficial ownership transparency

BOT on its own cannot necessarily mitigate the threats discussed, but BO data can be combined with other data sources to help with the enforcement of legislation designed to address these issues. It will be critical for these data to be structured and interoperable for this to be effective. For example, legislation to counter the buying of political influence may require a register of people and companies who lobby governments, as is the case under the US Foreign Agents Registration Act (FARA), which requires foreign lobbyists to register, or Australia's Foreign Influence Transparency Act. These datasets would be most effective if linked to other publicly available datasets, such as politicians' asset declarations and BO information.[99]

n Foreign nationals are barred from donating to US political candidates or committees. See: Lachlan Markay, "FEC lets foreigners finance U.S. ballot fights", *Axios*, 2 November 2021, https://www.axios.com/fec-foreign-money-referendum-dcc92322-05ad-4093-8bb8-35446ef6c964.html

Similarly, legislation requiring the disclosure of information about political parties and campaign financing can be combined with BOT to protect the integrity of political processes and improve citizens' trust in them. As the UK example above shows, it is critical for all relevant entities to be covered within the scope of disclosure.[100] This may also require complementary measures, such as extending due diligence requirements to a range of other businesses, including "law and public relations firms, investment and real estate advisors, and art dealers."[101]

The topics of legislating against the spread of disinformation and regulating social media campaign financing are being discussed by a number of countries in the context of disinformation around the COVID-19 pandemic.[o] Following criticism that the network's ads were used to influence the 2016 US elections, Facebook launched the Ad Library in 2019, which now includes "information from the advertiser" and "paid for by" information, including individuals' or companies' names.[102] However, there are no other identifiers besides a name for both individuals and companies, meaning it would be difficult to disambiguate similar names. The EU, in December 2020, proposed the Digital Services Act which would implement transparency obligations for online advertisements, including information on whose behalf ads are displayed.[103] Information to be provided will include "the identity and place of establishment of the sponsor on behalf of whom the advertisement is disseminated including their name, address, telephone number and electronic mail address, and whether they are a natural or legal entity".[104] In combination with public BO registers mandated under the AMLD5, this effectively provides BO information for political advertising. If social media networks published information about who pays for advertising campaigns as structured data with identifiers, this could be more easily connected to BO datasets from central public registers with structured and interoperable data.

---

o For example, only 12 social media accounts were found to be responsible for the vast majority of COVID-19 disinformation, which was named as a driving force behind the virus spreading. See: Erum Salam, "Majority of Covid misinformation came from 12 people, report finds", *The Guardian*, 17 July 2021, https://www.theguardian.com/world/2021/jul/17/covid-misinformation-conspiracy-theories-ccdh-report; Davey Alba and Sheryl Gay Stolberg, "Surgeon General Assails Tech Companies Over Misinformation on Covid-19", *The New York Times*, 12 September 2021, https://www.nytimes.com/2021/07/15/us/politics/surgeon-general-vaccine-misinformation.html.

Conclusion

The December 2020 US commitment to implementing a central BO register has put the spotlight on how BOT can contribute to national security. Mostly, this covers the use of BO data in known policy areas, rather than new ones.

BO data is essential in order to know with whom one is doing business. Anonymously owned shell companies are a significant loophole in legislation protecting national security, and can make countries complicit in illegal activities outside their jurisdiction that negatively impact their national security. These loopholes can be exploited by hostile states as part of foreign policy to undermine national security, or by actors pursuing financial incentives, for whom undermining national security is not the aim but whose actions undermine it nonetheless.

This briefing shows that the issue of national security cross-cuts a number of different policy areas where the use of BO information is relevant. It demonstrates that in order for BOT to address the loopholes, reliable and usable BO data needs to be made available in a timely manner to and used by a range of government and non-government actors. The most effective way to do this is through implementing central registers. In many instances, making the data available to the public can have further benefits.[105] For many of the policy areas, foreign state ownership of companies is relevant and should therefore be captured as part of BO disclosures in a standardised way.[106] All relevant entities should be included within the scope of disclosure.[107]

The briefing has also demonstrated that BO data is most valuable when combined with other data to enforce legislation, for instance, with government licensing data or lobbyist data. In order to do so efficiently, and in order to build in automated checks that can raise red flags, BO data should be made available as structured and interoperable data.[108] Beyond specific use cases, BOT provides visibility and knowledge of who is operating in an economy and financial system, which is a fundamental piece of information for knowing how best to protect it.

The OO Principles provide a framework for implementing comprehensive BOT reforms, in line with the recommendations set out in this briefing. They seek to generate actionable and usable data across the widest range of policy applications of BO data. Effective disclosure needs high quality, reliable data to maximise usability for all potential users and to minimise loopholes.[109]

Endnotes

1 See, for example: "9-90.010 - National Security", US Department of Justice, n.d., https://www.justice.gov/jm/jm-9-90000-national-security#9-90.010; Tang Aijun, "Ideological Security in the Framework of the Overall National Security Outlook", Central Party School of the Chinese Communist Party, Socialism, No. 5 (May 2019), http://socialismstudies.ccnu.edu.cn/bencandy.php?fid=71&id=1985; "The National Security Strategy of the United Kingdom", UK Cabinet Office, March 2008, 3-4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf; Samuel M. Makinda, "Sovereignty and Global Security", Security Dialogue 29, no. 3, September 1998, 281-292; Jude Blanchette, "Ideological Security as National Security", Center for Strategic and International Studies, 2 December 2020, https://www.csis.org/analysis/ideological-security-national-security.

2 Joseph R. Biden Jr., "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest", The White House, 3 June 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/memorandum-on-establishing-the-fight-against-corruption-as-a-core-united-states-national-security-interest/.

3 Ibid.

4 "Second interim report on the inquiry into the conduct of the 2016 federal election: Foreign Donations", Commonwealth of Australia, March 2017, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2016Election/Report_1.

5 Ieva Dunčikaitė, Jorge Valladares, and Deimantė Žemgulytė, "Paying for Views: Solving transparency and accountability risks in online political advertising", TI, 2021, https://images.transparencycdn.org/images/2021_Report_PayingForViews-OnlinePoliticalAdvertising_English.pdf.

6 In all these instances, there are additional benefits that arise from making central registers available to the public. See: Tymon Kiepe, "Making central beneficial ownership registers public", May 2021, OO, https://www.openownership.org/resources/making-central-beneficial-ownership-registers-public/; "Worldwide commitments and action", Open Ownership, n.d., https://www.openownership.org/map/.

7 Ian Michael Oxnevad, Making a Killing: States, Banks, and Terrorism (Montreal: McGill-Queen's Press, 2021), 16.

8 Ibid, 17.

9 Arun Advani, Emma Chamberlain, and Andy Summers, "A wealth tax for the UK", Wealth Tax Commission, 2020, https://www.wealthandpolicy.com/wp/WealthTaxFinalReport.pdf.

10 Tymon Kiepe and Eva Okunbor, "Beneficial ownership data in procurement", OO, March 2021, https://www.openownership.org/resources/beneficial-ownership-data-in-procurement/.

11 Tymon Kiepe and Sadaf Lakhani, "The use of beneficial ownership data by private entities", OO, forthcoming.

12 "Disclosing beneficial ownership", EITI, May 2017, https://eiti.org/files/documents/eiti_bo_factsheet_en_final.pdf.

13 Eric Edelman, Kristofer Harrison, Celeste Ward Gventer, and Philip Zelikow, "The Rise of Strategic Corruption: How States Weaponize Graft", Foreign Affairs, July/August 2020, https://www.foreignaffairs.com/articles/united-states/2020-06-09/rise-strategic-corruption.

14 "The Open Ownership Principles – Sufficient detail"; Jack Lord, "State-owned enterprises and beneficial ownership disclosures", OO, October 2021, https://www.openownership.org/blogs/state-owned-enterprises-and-beneficial-ownership-disclosures/.

15 See, for instance: Edda Müller et al., "Corruption as a Threat to Stability and Peace", TI, February 2014, https://ti-defence.org/wp-content/uploads/2016/03/2014-01_CorruptionThreatStabilityPeace.pdf.

16 "Why corruption matters: understanding causes, effects and how to address them", Department of International Development, January 2015, 51, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/406346/corruption-evidence-paper-why-corruption-matters.pdf.

17 See, for instance: Sarah Chayes, Thieves of State: Why Corruption Threatens Global Security, (London: W.W. Norton & Company Ltd., 2016).

18 Jorum Duri, "Corruption and economic crime", TI, 15 March 2021, 1, https://knowledgehub.transparency.org/assets/uploads/kproducts/2021-Corruption-and-economic-crime_final.pdf.

19 "Transnational Organized Crime: A Growing Threat to National and International Security", The White House, National Security Council, n.d., https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat.

20 "National risk assessment of money laundering and terrorist financing 2020", HM Treasury and Home Office, December 2020, 26, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf.

21 "National risk assessment of proliferation financing", HM Treasury, September 2021, 2, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020695/National_risk_assessment_of_proliferation_financing.pdf.

22 See: Agustin Armendariz et al., "Pandora Papers: An offshore data tsunami", ICIJ, 2 October 2021, https://www.icij.org/investigations/pandora-papers/about-pandora-papers-leak-dataset/; Emile van der Does de Willebois et al., "The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It", StAR, UNODC, and World Bank, 2011, https://star.worldbank.org/sites/star/files/puppetmastersv1.pdf.

23 "National risk assessment of money laundering and terrorist financing 2020", 26.

24 For instance, the UK Bribery Act 2010 and US Foreign Corrupt Practices Act (FCPA) 1977.

25 "Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law", Office Journal of the European Union, 12 November 2018, 5, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN.

26 "FATF: About", FATF, n.d., https://www.fatf-gafi.org/about/.

27 "Transnational Organized Crime: A Growing Threat to National and International Security".

28 Biden Jr., "Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest".

29 See, for instance: Petrus C. van Duyne, Jackie H. Harvey, Liliya Y. Gelemerova, The Critical Handbook of Money Laundering: Policy, Analysis and Myths, (London: Palgrave Macmillan), 2018.

30 Federico Mor and Ali Shalchi, "Registers of beneficial ownership", The House of Commons Library, 8 February 2021, 8, https://researchbriefings.files.parliament.uk/documents/CBP-8259/CBP-8259.pdf; Kiepe, "Making central beneficial ownership registers public", 5-6.

31 "The Open Ownership Principles – Public access", OO, July 2021, https://www.openownership.org/principles/public-access/; "The Open Ownership Principles – A central register", OO, https://www.openownership.org/principles/central-register/; Kiepe, "Making central beneficial ownership registers public".

32 Richard K. Gordon, On the Use and Abuse of Standards for Law: Global Governance and Offshore Financial Centers, 88 N.C. L. REV. 501, 577 (2010).

33 Baker McKenzie, Mark Simpson, and Richard Powell, "Money laundering: EU responds to terrorist financing and the Panama papers affair", Thomson Reuters, 26 July 2018, https://uk.practicallaw.thomsonreuters.com/w-015-8858.

34 Dennis Lormel, "Lessons Learned from the Paris and Brussels Terrorist Attacks", 29 March 2016, ACAMS Today, https://www.acamstoday.org/lessons-learned-paris-brussels-attacks/; "In the spotlight: How the EU is combatting terrorist financing", European Comission, 29 March 2016, https://ec.europa.eu/newsroom/fisma/items/29693/en.

35 Gordon, "A Tale of Two Studies: The Real Story of Terrorism Finance".

36 "Financial challenge to crime and terrorism", HM Treasury, February 2007, https://www.loc.gov/item/2008428851/.

37 "National risk assessment of money laundering and terrorist financing 2020", 44; Lormel, "Lessons Learned from the Paris and Brussels Terrorist Attacks"; Uche Igwe, "We must understand terrorist financing to defeat Boko Haram and Nigeria's insurgents", London School of Economics (blog), 3 August 2021, https://blogs.lse.ac.uk/africaatlse/2021/08/03/terrorist-financing-economy-defeat-boko-haram-nigeria-insurgents/.

38 "Van bank tot rechtbank, hoe effectief is de bestrijding van terrorismefinanciering?", University of Amsterdam, 23 November 2021, https://www.uva.nl/shared-content/faculteiten/nl/faculteit-der-maatschappij-en-gedragswetenschappen/nieuws/2021/11/hoe-effectief-is-de-bestrijding-van-terrorismefinanciering.html?cb.

39 Peter Neumann, "Don't Follow the Money: The Problem With the War on Terrorist Financing", Foreign Affairs, July/August 2017, https://www.foreignaffairs.com/articles/2017-06-13/dont-follow-money.

40 "'De-risking' within MONEYVAL states and territories", MONEYVAL, 15 April 2015, https://rm.coe.int/report-de-risking-within-moneyval-states-and-territories/168071510a; "Mitigating the effects of de-risking in emerging markets to preserve remittance flows", IFC, November 2016, https://openknowledge.worldbank.org/bitstream/handle/10986/30348/110883-BRI-Note-22-EMCompass-De-Risking-and-Remittances-FINAL-PUBLIC.pdf.

41 Oxnevad, Making a Killing: States, Banks, and Terrorism, 6.

42 For instance: Julia Morse, "The Counterterror War That America Is Winning", The Atlantic, 15 September 2021, https://www.theatlantic.com/ideas/archive/2021/09/america-terrorism-finance/620067/.

43 "FARC's Elusive Finances Undercut Support for Colombia Peace", VOA, 13 June 2017, https://www.voanews.com/a/farc-elusive-finances-undercut-support-colombia-peace/3899184.html; "Sanctions Programs and Country Information", U.S. Department of the Treasury, 2021, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/farc_net_08262009.pdf.

44 Enforcement can be ineffective where it is at odds with domestic national security priorities. See: Oxnevad, Making a Killing: States, Banks, and Terrorism, 6.

45 Yew Lun Tian, "China passes law to counter foreign sanctions", Reuters, 10 June 2021, https://www.reuters.com/world/china/china-passes-law-counter-foreign-sanctions-2021-06-10/.

46 "FCM Trust", Oil & Gas Authority, n.d., https://itportal.ogauthority.co.uk/eng/fox/oga-report/PED301X/companyBlocksDisplay?COMPANY_GROUP_ID=8160.

47 "US unleashes sanctions on Iran, hitting oil, banking and shipping", BBC, 5 November 2018, https://www.bbc.co.uk/news/business-46092435.

48 "Iranian Oil Company (U.K.) Limited", Companies House, 2021, https://find-and-update.company-information.service.gov.uk/company/01019769/persons-with-significant-controlfiling-history.

49 "Annual Report and Audited Financial Statements for the Year Ended 31 December 2020 for Iranian Oil Company (U.K.) Limited", Companies House, 2020, https://find-and-update.company-information.service.gov.uk/company/01019769/filing-history/MzMxNTExMDc3NmFkaXF6a2N4/document?format=pdf&download=0.

50 "SECTION 13(r) DISCLOSURES: Exhibit 99.1", US Securities and Exchange Commission", n.d., https://www.sec.gov/Archives/edgar/data/61398/000006139819000021/a33119ex-991.htm.

51 "Iranian Nationals Charged with Conspiring to Evade U.S. Sanctions on Iran by Disguising $300 Million in Transactions Over Two Decades", the United States Department of Justice, Office of Public Affairs, 19 March 2021, https://www.justice.gov/opa/pr/iranian-nationals-charged-conspiring-evade-us-sanctions-iran-disguising-300-million.

52 Joe Byrne, "The Shell Game", Nuclear Reactions, RUSI, https://www.nuclearreactions.rusi.org/single-post/2020/03/20/the-shell-game.

53 For examples of sanctions evasions using vessels, see: "U.S. Government Seizes Oil Tanker Used To Violate U.S. And U.N. Sanctions Against North Korea", the United States Department of Justice, U.S. Attorney's Office, 23 April 2021, https://www.justice.gov/usao-sdny/pr/us-government-seizes-oil-tanker-used-violate-us-and-un-sanctions-against-north-korea and "US seizes tanker used to deliver oil to North Korea", News24, 31 July 2021, https://www.news24.com/news24/world/news/us-seizes-tanker-used-to-deliver-oil-to-north-korea-20210731.

54 "Principles for Effective Beneficial Ownership Disclosure", OO, n.d., https:// www.openownership.org/principles/.

55 "The Open Ownership Principles – Sufficient detail".

56 "FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration", GAO Highlights, March 2020, 1, https://www.gao.gov/assets/gao-20-164-highlights.pdf.

57 "FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration", GAO, March 2020, 72-73, https://www.gao.gov/assets/gao-20-164.pdf.

58 "FAA Needs to Better Prevent, Detect, and Respond to Fraud and Abuse Risks in Aircraft Registration", GAO Highlights, 1.

59 Sandeep Mehta, "COVID-19 crisis inspires global tightening of Foreign Investment Screening", Norton Rose Fulbright, May 2020, 2, https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/global-rules-on-foreign-direct-investment/global-rules-on-foreign-direct-investment---india.pdf.

60 "Wet veiligheidstoets investeringen, fusies en overnames", Tweede Kamer der Staten-Generaal, 30 June, 2021, https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2021Z12360&dossier=35880.

61 "News Update Competition: Dutch FDI screening bill 2.0 sent to Parliament", Houthoff, 6 July 2021, https://www.houthoff.com/insights/News-Update/Competition-News-Update-6-July-2021.

62 "New and improved National Security and Investment Act set to be up and running", Department for Business, Energy & Industrial Strategy, 20 July 2021, https://www.gov.uk/government/news/new-and-improved-national-security-and-investment-act-set-to-be-up-and-running.

63 "National Security and Investment Act: prepare for new rules about acquisitions", Department for Business, Energy & Industrial Strategy, 20 July 2021, https://www.gov.uk/guidance/national-security-and-investment-act-guidance-on-acquisitions.

64 Natalia Zinets, "Ukraine's assembly backs law to rein in oligarchs in first reading", Reuters, 1 July 2021, https://www.reuters.com/world/europe/ukraines-assembly-backs-law-rein-oligarchs-first-reading-2021-07-01/; Polina Ivanova and Mark Raczkiewycz, "Ukraine passes law to curb political influence of oligarchs", Financial Times, 23 September 2021, https://www.ft.com/content/b9dbdbf1-7337-42e8-98f6-5a062c084e81. Whilst the law was meant to encourage legal pluralism, critics allege the opposite has happened. See: David Clark, "Ukraine's anti-oligarch law could make President Zelenskyy too powerful", Atlantic Council, November 6 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-anti-oligarch-law-could-make-president-zelenskyy-too-powerful/.

65 Miguel Franco T Dimayacyac and Rose Marie M. King-Dominguez, "In brief: media law and regulation in Philippines", SyCip Salazar Hernandez & Gatmaitan, 5 August 2020, https://www.lexology.com/library/detail.aspx?g=2c8a14b6-742a-40f7-b587-1aef8c77c420.

66 See, for instance, this case of media ownership that was traced back to Indonesia: "Philippines", Media Ownership Monitor, 20 November 2018, https://www.mom-rsf.org/en/countries/philippines/.

67 Mehta, "COVID-19 crisis inspires global tightening of Foreign Investment Screening", 1.

68 See: Kiepe, "Making central beneficial ownership registers public".

69 "The Open Ownership Principles – Sufficient detail", July 2021, OO, https://www.openownership.org/principles/sufficient-detail/.

70 OECD, OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials, (Paris: OECD Publishing, 2014).

71 Eva Anderson and Matthew T. Page, "Weaponising transparency: Defence procurement reform as a counterterrorism strategy in Nigeria" CISLAC, TI, and TI-DS, May 2017, 1, https://ti-defence.org/wp-content/uploads/2017/05/Weaponising_Transparency_Web.pdf.

72 Ibid, 15.

73 "Review into the risks of fraud and corruption in local government procurement: A commitment from the UK Anti-Corruption Strategy 2017-2022", UK Ministry of Housing, Communities and Local Government, June 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/890748/Fraud_and_corruption_risks_in_local_government_procurement_FINAL.pdf.

74 "Why corruption matters: understanding causes, effects and how to address them", UK Department for International Development, January 2015, 50, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/406346/corruption-evidence-paper-whycorruption-matters.pdf.

75 "Defense Procurement: Ongoing DOD Fraud Risk Assessment Efforts Should Include Contractor Ownership", GAO, November 2019, https://www.gao.gov/assets/710/702890.pdf.

76 "Aventura et al Complaint", Department of Justice, Eastern District of New York, n.d., https://www.justice.gov/usao-edny/press-release/file/1215951/download#page=8.

77 Rachael Hanna, "Shell Corporations Facilitate Contracting Fraud at the Department of Defense", Lawfare, 21 April 2020, https://www.lawfareblog.com/shell-corporations-facilitate-contracting-fraud-department-defense.

78 "GSA Should Inform Tenant Agencies When Leasing High-Security Space from Foreign Owners", GAO Highlights, January 2017, 1, https://www.gao.gov/assets/gao-17-195-highlights.pdf.

79 "GSA Should Inform Tenant Agencies When Leasing HighSecurity Space from Foreign Owners", GAO, January 2017, 20, https://www.gao.gov/assets/gao-17-195.pdf.

80 "WP1502: Beneficial ownership transparency and open contracting and public procurement (comments from Anti-Corruption Summit)", Wilton Park, 2016, https://www.wiltonpark.org.uk/wp-content/uploads/WP1502-Comments-on-beneficial-ownership-transparency-and-open-contracting-and-public-procurement-at-Anti-Corruption-Summit.pdf; "IMF COVID-19 Anti-Corruption Tracker", TI, 20 September 2020, https://www.transparency.org/en/imf-tracker.

81 Kiepe and Okunbor, "Beneficial ownership data in procurement", 11-12.

82 Ibid.

83 For instance, in Slovakia. See: Tymon Kiepe, Victor Ponsford, and Louise Russell-Prywata, "Early impacts of public registers of beneficial ownership: Slovakia", OO, September 2020, https://www.openownership.org/resources/early-impacts-of-public-registers-of-beneficial-ownership-slovakia/.

84 Dominic Cruz Bustillos, Matthew H. Murray, and Alexander Vindman, "Assessing the Threat of Weaponized Corruption", Lawfare, 7 July 2021, https://www.lawfareblog.com/assessing-threat-weaponized-corruption.

85 Edelman, Harrison, Ward Gventer, and Zelikow, "The Rise of Strategic Corruption: How States Weaponize Graft".

86 For instance, in the UK. See: "Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy", HM Government, March 2021, 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

87 See, for example: Special Counsel Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election", the United States Department of Justice, March 2019, https://www.justice.gov/archives/sco/file/1373816/download. These concerns have been mostly voiced by democratic countries which claim these activities are coordinated by hostile states.

88 Robert Gates, From the Shadows: The Ultimate Insider's Story of Five Presidents and How They Won the Cold War (New York: Simon & Schuster, 2007), quoted in Matthew Rosenberg, "With Bags of Cash, C.I.A. Seeks Influence in Afghanistan", The New York Times, 28 April 2013, https://www.nytimes.com/2013/04/29/world/asia/cia-delivers-cash-to-afghan-leaders-office.html.

89 Quoted from: Lord Evans of Weardale, "Regulating Election Finance", Committee on Standards in Public Life, July 2021, 48, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/999636/CSPL_Regulating_Election_Finance_Review_Final_Web.pdf; referencing: "Russia", Intelligence and Security Committee of Parliament, 21 July 2020, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf.

90 Adam Bychawski and Seth Thévoz, "Urgent changes needed to tackle dirty money in British politics, says new report", openDemocracy, 7 July 2021, https://www.opendemocracy.net/en/dark-money-investigations/urgent-changes-needed-tackle-dirty-money-british-politics-says-new-report/.

91 "FinCEN Files: Tory donor Lubov Chernukhin linked to $8m Putin ally funding", BBC, 21 September 2020, https://www.bbc.co.uk/news/uk-54228079.

92 "Report of the Select Committee on Intelligence – United States Senate On Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views", 116th Congress 1st Session Senate, Report 116-XX, United States Congress, October 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

93 Sir Robert Owen, "The Litvinenko Inquiry: Report into the death of Alexander Litvinenko", January 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/493860/The-Litvinenko-Inquiry-H-C-695-web.pdf.

94 Cruz Bustillos, Murray, and Vindman, "Assessing the Threat of Weaponized Corruption".

95 See, for instance: "Illicit Influence – Part One – A Case Study of the First Czech Russian Bank", Alliance for Securing Democracy and C4ADS, 28 December 2018, https://securingdemocracy.gmfus.org/first-czech-russian-bank-case-study/.

96 Hilmar Schmundt, "Was die neuen Corona-Medikamente können – und was nicht", Der Spiegel, 15 December 2021, https://www.spiegel.de/international/germany/documents-link-afd-parliamentarian-to-moscow-a-1261509.

97 Lord Evans of Weardale, "Regulating Election Finance", 6.

98 Bychawski and Thévoz, "Urgent changes needed to tackle dirty money in British politics, says new report".

99 Carl Dolan and Iskra Kirova, "Framing Paper: How the EU and US can disrupt Russia's corrupt economic statecraft", Center for a New American Security (CNAS) Transatlantic Forum on Russia, Anti-Corruption Working Group, 28 October 2021,10.

100 "The Open Ownership Principles – Comprehensive coverage", OO, July 2021, https://www.openownership.org/principles/comprehensive-coverage/.

101 "Representatives Malinowski, Salazar, Cohen and Wilson Introduce Bipartisan Legislation to Stop Enablers of International Corruption", United States House of Representatives: Congressman Tom Malinowski, press release, 6 October 2021, https://malinowski.house.gov/media/press-releases/representatives-malinowski-salazar-cohen-and-wilson-introduce-bipartisan.

102 Josh Constine, "Facebook launches searchable transparency library of all active ads", TechCrunch, 28 March 2019, https://techcrunch.com/2019/03/28/facebook-ads-library/.

103 "The Digital Services Act package", European Commission, 21 October 2021, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

104 "Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising", European Commission, 25 November 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0731.

105 Kiepe, "Making central beneficial ownership registers public".

106 "The Open Ownership Principles – Sufficient detail"; Jack Lord, "State-owned enterprises and beneficial ownership disclosures", OO, October 2021, https://www.openownership.org/blogs/state-owned-enterprises-and-beneficial-ownership-disclosures/.

107 "The Open Ownership Principles – Comprehensive coverage".

108 The Open Ownership Principles – Structured data", OO, July 2021, https://www.openownership.org/principles/structured-data/.

109 "Principles for Effective Beneficial Ownership Disclosure".

Author
Tymon Kiepe

with contributions by
Alanna Markle
Peter Low
Thom Townsend

Editor
Cara Marks

Reviewers
Anton Moiseienko (Australian National University)
Matthew Jenkins (Transparency International)

Design
Convincible Media

Cover
Photo by Michael Afonso on Unsplash

Open Ownership

openownership.org
@openownership
c/o Global Impact, 1199 North Fairfax Street, Suite 300, Alexandria, VA 22314, USA