www.rusi.org

Occasional Paper

Developing Bad Habits
What Russia Might Learn from Iran's Sanctions Evasion

Tom Keatinge

Occasional Paper

192 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, June 2023. ISSN 2397-0286 (Online).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The author would like to thank Matthew Redhead for the considerable literature review he provided for this paper, alongside Stephen Reimer, Senior Research Fellow, for his contribution to this paper. He would also like to thank Gonzalo Saiz, Research Analyst, for additional research support, and as ever, the RUSI Publications team for their diligent support and guidance.

Executive Summary

As Western nations and their allies across the globe impose a growing raft of sanctions on the Russian economy, evidence is emerging of adaptations in Russia's financial and trade strategy. Examples include the switching of ownership of companies and properties to family members or affiliates, the use of trading companies to source foreign exchange to avoid the sanctions imposed on the Central Bank of Russia, and import substitution, which the country has adopted since it was first targeted by Western sanctions in 2014. Alongside these steps, Russia is now gravitating further towards other states that have faced similarly sweeping restrictive measures or that facilitate sanctions evasion, to learn best practice, secure necessary services and establish trade relationships.

By highlighting the experience of other rogue states, this paper examines the question of how Western governments, notably in Europe, and their private sectors could strengthen their sanctions implementation and enforcement strategies in light of potential changes in Russia's financial activity. In particular, the paper considers techniques that Russia might learn from rogue states to create a similar – or interconnected – parallel financial system.

In this regard, Iran represents a notable case study. The country has faced financial sanctions from the international community for years, seeks to fund its economy through the export of hydrocarbons, and has most recently had to adapt to the reimposition of sanctions by the US, following former US president Donald Trump's withdrawal from the 2015 nuclear deal (the Joint Comprehensive Plan of Action), under which Iran originally received certain UN, unilateral and national sanctions reliefs related to its nuclear programme.

Iran also demonstrates the kinds of symbiotic relationships (or mutually beneficial commercial partnerships) between rogue states and non-state actors (including designated terrorist groups) that can benefit from the move to clandestine finance systems. For example, Iran's funding and resourcing of Hizbullah is reciprocated in numerous ways, including through support for the state's intermediary oil trading schemes. Such joint ventures or marriages of convenience between rogue states and their proxies may possibly be mirrored in the ways in which private military companies patronised by Russia advance Russian interests (and enable the circumvention of sanctions) globally.

To facilitate its trade and finance ambitions, Iran also co-opts service-providing states, such as financial centres, where supervision and enforcement of financial crime regulations is weak.

While evidence has yet to emerge of the complete adaptation of the financial systems needed by Russia to run its economy in defiance of allied sanctions, given the likely prolonged isolation of Russia from the international financial system, similar to Iran, it can be expected that it will seek to establish parallel financial relations that seek to evade the sanctions set against it by Ukraine's allies.

Introduction

The underlying logic of the use of sanctions measures is coercion through economic restriction. If a state cannot sell goods and services to generate hard international currencies or cannot use such currencies to buy the items it needs to sustain its activities or support its regime, then eventually – the theory goes – that state will need to reconsider its course of action. To beat sanctions, therefore, targeted states need to find ways to sustain domestic economic activity and trade.

Iran has been subject to some form of economic sanction since 1979. The country has had decades in which to develop finance and trade networks that facilitate the evasion of Western sanctions, from those banning Iranian imports to the US following the 1979 hostage crisis through the US designation of Iran as a state sponsor of terrorism in 1984 and a range of nuclear-related UN Security Council sanctions resolutions in the early 2000s to the more recent reimposition and ramping up of sanctions under former president Donald Trump's 'maximum pressure' campaign following the US withdrawal from the Joint Comprehensive Plan of Action (JCPOA)[1] in May 2018. Other countries have likewise developed mechanisms for evading Western sanctions. North Korea has established networks and structures for continuing to source the materials and funding it needs to pursue its ambition to develop its nuclear programme; Venezuela has similarly facilitated the export of oil in contravention of US sanctions; and countries as diverse as Sudan, Yemen and Zimbabwe have similarly grappled with evading the sanctions net imposed by the US, the EU or their allies that dominate the global financial system.

But, with an economy estimated to be worth US$90 billion,[2] and a need to export its oil and import the goods required to support its domestic and military economies, it is Iran that has developed the most sophisticated and wide-reaching mechanisms. Such mechanisms seek to allow it to operate beyond the reach of Western economic sanctions and the financial systems controlled by the US, the UK and the EU. This is particularly so since the collapse – in essence – of the JCPOA. This deal, struck in 2015, provided certain nuclear-related sanctions reliefs to Iran which, when Trump removed his support for the deal in 2018, saw

1. 'Joint Comprehensive Plan of Action', 14 July 2015, <https://eeas.europa.eu/archives/docs/statements-eeas/docs/iran_agreement/iran_joint-comprehensive-plan-of-action_en.pdf>, accessed 12 February.
2. World Bank, 'Islamic Republic of Iran', <https://www.worldbank.org/en/country/iran/overview>, accessed 8 January 2023.

sanctions on Iran 'snap back'.[3] Although the remaining signatories to the deal sought to sustain it via negotiation and financial engineering, the latter an attempt to facilitate continued trade with Iran in the face of US sanctions, the dominance of the US and the US dollar in global trade and finance has neutered these efforts.

Against this background, since Russia's full-scale invasion of Ukraine in February 2022, Western officials have expressed concerns over Russia's growing proximity to Iran and other rogue states, and the impact of these relationships on the future of the international order.[4] One anticipated development is that these states – all subject to sanctions regimes – will share lessons on how to avoid restrictive measures and abuse the international financial system for their own malign purposes.[5]

Until February 2022, for most parts of the global financial and economic system, Russia represented a business and profit-making opportunity. Since the Kremlin's full-scale invasion of Ukraine, this position has, of course, rapidly reversed as wide-ranging sanctions have been imposed on the Russian economy and financial system. This reversal of integration has presented challenges that will require Western allies to pay detailed attention to any ongoing economic connection with Russia, while at the same time, the Kremlin will face the challenge of maintaining both its civilian and military supply chains in the face of the rupturing of previously reliable funding and resourcing connections.

This paper seeks to answer the question: how should Western governments, notably those in Europe, and their private sectors strengthen their sanctions implementation and enforcement to counter changes in Russia's financial activity that have been borrowed from rogue states?

The paper has four chapters. Chapter I reviews the key measures taken by the international community to restrict the financial activity of rogue states and assess the various means by which these states have sought to blunt these efforts. To illustrate these concepts in more detail, the case of Iran is used in Chapter II to detail particular activities that may be relevant to the newest member of the rogue state club, Russia. Chapter III focuses on Russia and why and how these tools may be relevant as Western sanctions in response to Russia's war of

3. *The Guardian*, 'Donald Trump Vows "Snapback" Over Humiliating UN Defeat on Iran Arms Embargo', 16 August 2020.
4. Elsa Maishman and Sam Hancock, 'Ukraine War: US Says Iran Now Russia's "Top Military Backer"', *BBC News*, 11 December 2022.
5. Matthew Karnitschnig, 'Iran Teaches Russia its Tricks on Beating Oil Sanctions', *Politico*, 9 November 2022, <https://www.politico.eu/article/iran-russia-cooperation-dodging-oil-sanctions/>, accessed 12 December 2022; Ian Talley, 'Clandestine Finance System Helped Iran Withstand Sanctions Crush, Documents Show', *Wall Street Journal*, 18 March 2022; Nikita Smagin, 'Comrades-in-Sanctions: Can Iran Help Russia Weather the Economic Storm?', Carnegie Endowment for International Peace, 11 April 2022.

aggression in Ukraine tighten and isolate the country from its traditional markets. Chapter IV considers the current weaknesses in the financial system that are exploited by rogue states. The paper concludes with recommendations for Western policymakers and those supervising and operating in the international financial system to refocus their efforts to ensure that they are equipped with the understanding and tools to blunt the effort of rogue states to finance their malign activities via alternative financial and economic systems, described by some – and in this paper – as 'clandestine finance systems' (CFSs).[6]

What emerges is a picture of varyingly complex CFSs with shared family characteristics, which use, among other techniques, overseas front companies and ledger systems to mask the financing and transacting of trade. Of particular concern, beyond the need to ensure that financial and economic restrictions placed on a country's activities to support international security objectives are implemented, is that this activity can also be used by rogue states to transfer funds to their proxies. As the example of Iran shows, the development of a CFS can provide new avenues for state-sponsored terrorist financing, and indeed can make a virtue of a necessity by actively involving the designated terrorist group in the management of a CFS. An analysis of the activities of Russia's private military company the Wagner Group suggests that such activity is clearly a very real possibility as Russia adapts to the pressure of international sanctions.[7]

Methodology

This paper is informed by a review of English-language open source literature on the evasion techniques used by countries currently under stringent sanctions imposed by the UN Security Council (UNSC) and/or coalitions of Western states. Specifically, this review was undertaken in the first quarter of 2023 and draws on material from official documents produced by international organisations such as the UN and the Financial Action Task Force (FATF), the global anti-money-laundering and counterterrorist-financing standard setter,[8] and national governments' institutions and agencies, such as the US Treasury's Office of Foreign Assets Control (OFAC), the US's main sanctions administrator.[9] It considers academic and policy research from online searches via Google and dedicated research databases such as EBSCO and JSTOR, and, in addition, reputable and

6. Talley, 'Clandestine Finance System Helped Iran Withstand Sanctions Crush, Documents Show'.
7. Miles Johnson, 'Wagner Leader Generated $250mn from Sanctioned Empire', *Financial Times*, 21 February 2023.
8. Financial Action Task Force (FATF), <https://www.fatf-gafi.org>, accessed 12 December 2022.
9. US Department of the Treasury, 'Office of Foreign Assets Control – Sanctions Programs and Information', <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>, accessed 12 December 2022.

corroborated media reporting. The research draws on credible leak databases, notably Wiki Iran,[10] and sources relied on by professionals in governments and the private sector to support their identification of sanctions evasion activity.

The research faced a number of constraints as there is limited open source information on the mechanics of CFSs. The operational effectiveness of CFSs requires those controlling them to protect ‘tradecraft’ secrets, and those agencies dedicated to interdicting them will be wary of sharing this knowledge publicly, if known, for fear of prompting a change in the target’s behaviour. This means that much of what is known relies heavily on the public statements of government agencies taking enforcement action (most commonly OFAC) or when an international organisation is mandated to provide a review of sanctions evasion activities (such as through one of the Panel of Experts (PoEs) tasked with reviewing the implementation of UNSC resolutions).[11] Bearing in mind the clandestine nature of this activity, interviews were only used to validate the credibility of certain sources, in particular Wiki Iran.[12]

Definitions and Terminology

The paper uses a number of terms which vary in use and novelty. ‘Rogue states’ was a phrase first used in 1994 by then US National Security Adviser Anthony Lake to describe countries which consistently flouted international standards and took an adversarial position towards the US and its allies.[13] This definition is used in this paper and applied to those states that are also subject to severe UNSC and/or Western bi- or multilateral sanctions as a result of their behaviour: Belarus, Iran, Myanmar, Nicaragua, North Korea, Russia, Syria, and Venezuela.

The term ‘clandestine finance system’ is new, and – notwithstanding its use in a 2022 *Wall Street Journal* article on Iran[14] – does not have wide currency in academic or policy debate. In this paper, it refers to a method, or set of methods, used by a government, government agency or a non-state actor to undertake illicit economic and/or financial activities without detection.

10. Wiki Iran is a website that ‘aims to expose the Islamic Republic of Iran’s violations of international laws and regulations’. The website claims to be managed by second-generation Iranians in exile with experience in ‘international law, finance, banking, medicine, media and computer and chemical engineering’, see <www.wikiran.org>, accessed 7 April 2023.
11. See, for example, UN Security Council, ‘Security Council Committee Established Pursuant to Resolution 1718 (2006)’, <https://www.un.org/securitycouncil/sanctions/1718>, accessed 9 May 2023.
12. Interviews with two senior financial crime experts in global institutions, January 2023.
13. Anthony Lake, ‘Confronting Backlash States’, *Foreign Affairs*, March/April 1994, <https://www.foreignaffairs.com/articles/iran/1994-03-01/confronting-backlash-states>, accessed 12 December 2022.
14. Talley, ‘Clandestine Finance System Helped Iran Withstand Sanctions Crush, Documents Show’.

For a third key term, 'terrorist financing', the paper draws on the work of contemporary researchers such as Jessica Davis, who define it as a set of financial activities – raising, using, storing, moving, managing and obscuring funds – undertaken to fulfil terrorist purposes, whether those purposes are operational, such as mounting attacks, or organisational, such as providing ongoing day-to-day support for the group or network.[15] In terms of terrorist financing, the paper focuses mainly on the raising and moving of funds from states to their terrorist dependents, while also discussing active and intentional state support for terrorist groups, rather than passive state support or negligence, which might allow terrorists or their supporters to conduct financing activities unimpeded. Although some researchers treat passive support as a form of 'state sponsorship of terrorism',[16] if included here it would potentially bring in several states for consideration not widely recognised as rogue states. A noted recent example would be Qatar, which was sanctioned by several of its regional neighbours from June 2017 to January 2021 for allegedly supporting terrorism and criticised – but not sanctioned – by the US for its failure to do enough to tackle terrorist fundraising more generally.[17]

15. Jessica Davis, *Illicit Money: Financing Terrorism in the Twenty-First Century* (Boulder, CO: Lynne Rienner, 2021), pp. 2–6.
16. Daniel L Byman, 'Confronting Passive Sponsors of Terrorism', Analysis Paper Number 4, Saban Center for Middle East Policy at the Brookings Institution, February 2005, pp. 1–2, <https://www.brookings.edu/wp-content/uploads/2016/06/byman20050201.pdf>, accessed 12 December 2022; Daniel L Byman, 'The Changing Nature of State Sponsorship of Terrorism', Analysis Paper Number 16, Saban Center for Middle East Policy at the Brookings Institution, May 2008, pp. 3–5, <https://www.brookings.edu/wp-content/uploads/2016/06/05_terrorism_byman.pdf>, accessed 12 December 2022.
17. Tom Keatinge, 'Why Qatar is the Focus of Terrorism Claims', *BBC News*, 13 June 2017; *Al Jazeera*, 'Saudi FM: Full Ties Restored Between Qatar and Blockading Nations', 5 January 2021, <https://www.aljazeera.com/news/2021/1/5/saudi-says-full-ties-restored-between-qatar-and-embargo-nations>, accessed 12 December 2022.

I. Targeting Rogue States

This chapter reviews the methods by which the international community has targeted the financial and economic activities of rogue states and how these states have responded.

There is a wide range of literature reviewing the use of sanctions, both in a historical context and considering more contemporary use from a policymaker perspective.[18] The private sector also produces extensive research on the topic in support of banks and other regulated sectors that are required to implement asset freezes under sanctions designations.[19] This chapter does not intend to revisit in detail this literature, but highlights why it is that rogue state CFSs have developed as a result.

Sanctions are most commonly deployed by states or groups of states facing national security challenges to coerce a state back to acceptable behaviour, or at the very least punish the regime of that state.[20] For example, the 2021 US Treasury Sanctions Review argues that the use of sanctions against Iran to prevent it from

> using the international financial system and commercial markets to generate revenue through oil sales and other activities that support its nuclear and ballistic missile proliferation and support for terrorist activities … pushed Iran to the negotiating table on its nuclear program in 2015.[21]

In the case of Iran, the review also claims that US sanctions 'so significantly impaired Hizballah funding streams that in 2019 the organization had to reduce salaries for its military arm and media efforts and publicly solicit donations'.[22]

---

18. Nicholas Mulder, *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War* (New Haven, CT and London: Yale University Press, 2022); Paul Einzig, *Economic Warfare, 1939–1940* (London: Macmillan, 1940); Richard Nephew, *The Art of Sanctions: A View from the Field* (New York, NY: Columbia University Press, 2018); Agathe Demarais, *Backfire: How Sanctions Reshape the World Against U.S. Interests* (New York, NY: Columbia University Press, 2022).
19. See, for example, Kharon, 'Regulatory & Policy Guidance on Managing Sanctions-Related Risk', February 2019, <https://brief.kharon.com/whitepapers/regulatory-policy-guidance-on-managing-sanctions-related-risk>, accessed 7 April 2023; LexisNexis Risk Solutions, 'Sanctions Screening: A Best Practice Guide', <https://risk.lexisnexis.co.uk/corporations-and-non-profits/financial-crime-compliance/watchlist-screening/sanctions-list-screening/sanctions-screening-guide>, accessed 7 April 2023.
20. Jonathan Masters, 'What are Economic Sanctions?', Council on Foreign Relations, 12 August 2019, <https://www.cfr.org/backgrounder/what-are-economic-sanctions>, accessed 12 December 2022.
21. US Department of the Treasury, 'The Treasury 2021 Sanctions Review', October 2021, p. 1, <https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf>, accessed 12 December 2022.
22. *Ibid*.

The most widely recognised sanctions are those issued by the UNSC, to which all 193 UN member states are required to adhere.[23] Outside the UN, there are also a growing number of autonomous sanctions regimes, including those of the US, the EU, Canada, the UK and Australia.[24] Of these, the most potent is that of the US, which uses the power and ubiquity of the US dollar in international trade not only to prevent its own nationals and businesses from engaging with designated targets (primary sanctions), but also on occasion those of other nations (secondary sanctions).[25]

The elements of these autonomous national regimes vary. Depending on the targeted country and the issuing authority, some of the most common areas of designation include: embargos on arms; military materiel and technology; trade and investment bans on key export/import sectors; and asset freezes and travel bans on individuals and entities linked to the regime or malign activities.[26] The Western allies' latest sanctions on Russia have gone further to also include prohibiting the use of airspace, roads and ports, and a ban on certain media outlets. There can also be asset freezes and bans on transactions for designated financial institutions, as well as restrictions on access to the infrastructure of international finance such as the SWIFT messaging system, currently affecting financial institutions in Iran (extensively) and Russia (partially).[27]

In sum, for states whose economies rely on access to international markets for trade (such as the sale and purchase of oil and other hydrocarbons) and finance, sanctions should pose a material restriction. Yet rogue states have agency, and the next section considers how these states might choose to respond.

---

23. UNSC, 'Sanctions', <https://www.un.org/securitycouncil/sanctions/information>, accessed 12 December 2022.
24. See, for example, Australian Government Department of Foreign Affairs and Trade, 'Australia and Sanctions', <https://www.dfat.gov.au/international-relations/security/sanctions>, accessed 12 December 2022; European Commission, 'Finance – Sanctions (Restrictive Measures)', <https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures_en>, accessed 12 December 2022; Government of Canada, 'Consolidated Canadian Autonomous Sanctions List', <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/consolidated-consolide.aspx?lang=eng>, accessed 12 December 2022; Foreign, Commonwealth & Development Office, 'The UK Sanctions List', <https://www.gov.uk/government/publications/the-uk-sanctions-list>, accessed 12 December 2022; US Department of the Treasury, Office of Foreign Assets Control, 'Sanctions Programs and Country Information', <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information>, accessed 12 December 2022.
25. Anshu Siripurapu, 'The Dollar: The World's Currency', Council on Foreign Relations, 29 September 2020, <https://www.cfr.org/backgrounder/dollar-worlds-currency>, accessed 12 December 2022; Jason Bartlett and Megan Ophel, 'Sanctions by the Numbers: U.S. Secondary Sanctions', Center for New American Security, 26 August 2021, <https://www.cnas.org/publications/reports/sanctions-by-the-numbers-u-s-secondary-sanctions>, accessed 12 December 2022.
26. Masters, 'What are Economic Sanctions?'.
27. *Ibid.*; Ben Chapman, 'What is SWIFT and Why Does it Matter?', *The Independent*, 27 February 2022; SWIFT, 'Compliance – SWIFT and Sanctions', <https://www.swift.com/about-us/legal/compliance-0/swift-and-sanctions>, accessed 12 December 2022.

Rogue State Responses

As noted, the underlying logic of these sanctions measures is coercion through economic restriction. If a country cannot sell goods and services to generate hard international currencies or cannot use such currencies to buy the items the state needs to sustain its activities or support its regime, then eventually – the theory goes – that state will need to reconsider its course of action. To beat sanctions, therefore, targeted states need to find ways to sustain domestic economic activity and trade.

The responses of rogue states to this predicament have been varied, although there has been a familiar rhetorical commitment to self-sufficiency from states such as South Africa during the apartheid era and Iraq after the first Gulf War in 1991. In 2007, Iran's Supreme Leader Ayatollah Ali Khamenei coined the term 'resistance economy',[28] a concept which has developed since into a programme of initiatives which include reduced consumption and waste and more efficient use of domestic economic resources.[29] Rogue states have also sought to continue economic interactions in commercial sectors where sanctions are more ambiguous. For many years, North Korea has sought to continue working between the cracks of UN sanctions, providing construction workers, medical services and other forms of cheap labour to sympathetic states, for example in sub-Saharan Africa.[30] Although the UNSC required UN members to repatriate all North Korean workers by 22 December 2019, UN PoE reports continue to suggest their presence overseas.[31]

Others have continued to trade openly in commodities that are subject to unilateral sanctions (for example, sanctions from the US or the EU), but not UN-backed sanctions. Russia has sought to work around the Western designations of its oil sales by finding new buyers among 'neutral' states such as China and India, who have not applied sanctions to Russia following its full-scale invasion of Ukraine.[32] A further area of open activity has been the negotiation of barter deals, which, by relying on the physical exchange of equally valued goods, potentially avoids points of contact with the US dollar or other international currencies where activity should be identified and blocked by the banking system. Such deals are

28. Hussain Abdul-Hussain, 'Iran's "Resistance Economy" hasn't Worked Before and it Won't Work Now', *Arab News*, 6 April 2021, <https://www.arabnews.com/node/1838666>, accessed 12 December 2022.
29. Bijan Khajehpour, 'Decoding Iran's "Resistance Economy"', *Al-Monitor*, 24 February 2014, <https://www.al-monitor.com/originals/2014/02/decoding-resistance-economy-iran.html>, accessed 12 December 2022.
30. Darya Dolzikova and Anagha Joshi, 'The Southern Stratagem: North Korean Proliferation Financing in Southern and Eastern Africa', *RUSI Occasional Papers* (April 2020), pp. 26–30.
31. UNSC Resolution 2371, 5 August 2017, S/RES/2371, para. 11, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/246/68/PDF/N1724668.pdf?OpenElement>, accessed 12 December 2022; UN 1718 Sanctions Committee PoE, 'Final Report of the Panel of Experts Submitted Pursuant to Resolution 2569 (2021)', 1 March 2022, S/2022/132, pp. 77–79, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/252/09/PDF/N2225209.pdf?OpenElement>, accessed 12 December 2022.
32. Shruti Menon, 'Ukraine Crisis: Who is Buying Russian Oil and Gas?', *BBC News*, 6 December 2022.

being attempted between sanctioned states, such as Iran and Venezuela, but also between sanctioned and neutral partners, such as Iran and Pakistan, since December 2021.[33] Heavily sanctioned states – Russia and Iran, for example – have also started denominating bilateral trade in their local currencies,[34] as well as looking to trade in non-Western currencies, such as the Chinese renminbi and UAE dirhams, as a form of alternative international settlement currency to the US dollar.[35] Last, to support the development on non-G7 currency trade, countries are establishing connected domestic currency settlement systems. For example, Russia and Iran are reportedly integrating both their national financial messaging systems[36] and their individual bank card networks (respectively called Mir and Shetab), which is expected to facilitate the de-dollarisation of financial transactions related to bilateral trade.[37]

33. Maziar Motamedi, 'Iran, Venezuela Sign 20-Year Cooperation Plan During Maduro Visit', *Al Jazeera*, 11 June 2022; *Express Tribune*, 'Pakistan, Iran to Increase Bilateral Trade to $5 Billion', 8 November 2021, <https://tribune.com.pk/story/2328389/pakistan-iran-to-increase-bilateral-trade-to-5-billion>, accessed 12 December 2022.
34. *Al-Monitor*, 'Iran, Russia Use Own Currencies for Trade', 24 August 2022, <https://www.al-monitor.com/originals/2022/08/iran-russia-use-own-currencies-trade>, accessed 12 December 2022.
35. *Bloomberg*, 'Russia Gives China's Yuan a Boost as Firms Cope with Sanctions', 14 September 2022, <https://www.bloomberg.com/news/articles/2022-09-14/yuan-s-clout-gets-a-boost-from-russia-trade-as-sanctions-bite?leadSource=uverify%20wall>, accessed 8 March 2023.
36. *Reuters*, 'Iran, Russia Link Banking Systems Amid Western Sanction', 30 January 2023.
37. *Financial Tribune*, 'Iran Can Join Russia's Mir Payment Network by Early 2023, Minister Says', 11 October 2022, <https://financialtribune.com/articles/business-and-markets/115504/iran-can-join-russia-s-mir-payment-network-by-early-2023>, accessed 12 December 2022; Michael Scollon, '"A Terrible Club to be in": Russia, Iran, and the Bloc of Sanctioned Nations', *Radio Free Europe Radio Liberty*, <https://www.rferl.org/a/russia-iran-sanctioned-states-burma-north-korea-belarus/32205382.html>, accessed 8 March 2023.

Case Study: The Asian Clearing Union (ACU)

As global trade becomes more fragmented under the pressure of sanctions and efforts by those subject to sanctions to circumvent the reach of the US dollar and other G7 currencies, as indicated earlier, advance barter trade is becoming more prominent. Barter trade is a form of exchange that has existed for millennia, but in the modern era its relevance has resurged in the face of national capital controls that restrict cross-border payments, and liquidity shortages created by bilateral payment clearing between nations.

As a result of these restrictions, various settlement systems have been developed that allow for payments to be 'netted', which means that where groups of countries trade with each other, only balancing payments – rather than gross payments – need to be made between central banks.

One such settlement forum is the ACU. Formed in 1974 at the initiative of the UN Economic and Social Commission for Asia and the Pacific, the ACU now comprises nine members, including Bangladesh, Bhutan, India, Iran, Maldives, Myanmar, Nepal, Pakistan, and Sri Lanka.

In essence, the ACU facilitates trade between the member nations without the need for payment beyond a final settlement payment. Such a structure is tailor-made to support sanctions evasion as it allows countries to trade without an accompanying financial transaction. While the ACU has accounts with the formal financial system to facilitate the netting of these 'IOUs' between countries, where a final balancing payment is needed, this payment can also be made in a local currency, avoiding the need to use the Western banking system. With the advent of central bank digital currencies, such balancing payments, made beyond the reach of Western authorities, are likely to become even easier.

Such settlement platforms, originally established to enhance regional trade, are likely to face a renaissance as countries face new financial system restrictions, this time caused by sanctions rather than liquidity or capital controls.

Source: Asian Clearing Union, 'ACU in Brief', <https://www.asianclearingunion.org/Home.aspx>, accessed 4 January 2023.

II. Iran’s Journey of Financial System Innovation

Against this outline of the different ways in which rogue states and those that facilitate their activity operate, this chapter considers the specific case of Iran.

Overt trade efforts with friends and neutrals are only one aspect of how sanctioned states continue to survive. Clandestine activities are also key. Facing the dominance of US dollar pricing in international trade, rogue states need to find ways to generate dollars they do not currently have, and ways to spend them. In the first half of the requirement – making money – two methods commonly appear: secretly converting domestic currency and assets; and generating funds through committing illicit acts.

Iran has a long history of seeking to respond to sanctions. It is beyond the scope of this paper to review this history, which has been addressed in detail by others.[38] This paper therefore considers contemporary examples, taken primarily from sanctions designations made by OFAC, to demonstrate the way in which Iran has used CFSs to operate its economy while under sanctions, specifically considering currency conversion and intermediary trading.

Currency Conversion

Currency conversion requires the physical transfer of domestic currency out of the rogue state, its conversion into physical US dollars, and its successful return. In recent years, the US has outlined publicly two such cases of currency conversion linked to Iran. In May 2018, OFAC revealed a scheme where the regime’s elite military unit, the Islamic Revolutionary Guard Corps (IRGC), transferred Iran’s domestic currency, the rial, in bulk to the UAE, where it was then converted into US dollars by complicit money exchange houses, an activity that was hidden from authorities through the creation of forged documentation.[39] In a further designation in September 2021, OFAC identified another scheme involving the IRGC, where

38. See, for example, Melina Helga Richter, *US Sanctions Against Iran: Historical Context, Goals and Consequences* (Munich: GRIN Verlag, 2020); Nephew, *The Art of Sanctions.*
39. US Department of the Treasury, ‘United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF’, 10 May 2018, <https://home.treasury.gov/news/press-releases/sm0383>, accessed 12 December 2022.

currency and gold were smuggled on commercial flights to Turkey operated by the Iranian airline Mahan Air, itself a US-designated carrier. Once the trade was completed, the currency and gold were sold via a complicit intermediary, and the proceeds were transferred by commercial flight back to Iran.[40]

Intermediary Trading

It is, however, unrealistic to expect bulk conversion of domestic currencies – or the increasingly reported use of cryptocurrencies[41] – to be feasible on the kind of scale necessary to support even a mid-sized economy such as Iran's, where imports and exports are valued in the tens of billions.[42]

Some rogue states, such as North Korea, supplement this approach by conducting illicit activities. Since the 1970s, North Korea has built up an extensive charge sheet, including the production and trafficking of illegal narcotics; the counterfeiting and trafficking of pharmaceuticals, cigarettes and US currency; and the smuggling and sale of high-value items, including precious metals, stones and illegal wildlife.[43] More recently, however, the North Korean state's direct involvement in some of these schemes has waned, most notably narcotics trafficking,[44] superseded by a focus on cybercrime, and in particular the theft of cryptocurrency. According to research by Chainalysis, a blockchain analytics firm, North Korean hackers stole the equivalent of US$400 million in cryptocurrencies in 2021,[45] a figure that will be far surpassed in 2022, following hacks that have included the theft in March of US$600-million worth of cryptocurrencies from online game platform Ronin Network's Axie Infinity

40. US Department of the Treasury, 'Treasury Sanctions International Financial Networks Supporting Terrorism', 17 September 2021, <https://home.treasury.gov/news/press-releases/jy0362>, accessed 12 December 2022.
41. Behnam Gholipour, 'Official Report: Iran Could Use Cryptocurrencies to Avoid Sanctions', *Iran Wire*, 2 March 2021, <https://iranwire.com/en/features/69084/>, accessed 12 December 2022.
42. World Bank, 'Exports of Goods and Services (Constant 2015 US$) – Iran, Islamic Republic', <https://data.worldbank.org/indicator/NE.EXP.GNFS.KD?end=2020&locations=IR&start=1960&view=chart>, accessed 12 December 2022.
43. Bruce E Bechtol Jr, 'North Korean Illicit Activities and Sanctions: A National Security Dilemma', *Cornell International Law Journal* (Vol. 57, No. 1, 2018), pp. 57–99; Sheena Chestnut Greitens, 'Illicit: North Korea's Evolving Operations to Earn Hard Currency', Committee for Human Rights in North Korea, 2014, <https://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf>, accessed 12 December 2022.
44. US Department of State Bureau for International Narcotics and Law Enforcement Affairs, 'International Narcotics Control Strategy Report Volume I: Drug and Chemical Control', March 2017, p. 143.
45. Chainalysis, 'The 2022 Crypto Crime Report', February 2022, p. 113, <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>, accessed 12 December 2022.

game.[46] A high proportion of these funds are reportedly cashed out over time into renminbi through offshore cryptocurrency exchanges.[47]

While converting domestic cash and generating illicit funds can make hard currency, neither provides an immediate way to use those funds to buy goods on the open market. A more sophisticated and dual-sided mechanism, allowing both the generation of funds and the means to spend them, is needed.

The solution that Iran has developed is to continue trading by hiding its activities behind intermediaries, or 'hidden subsidiaries', as senior Iranian official Gholamreza Mesbahi-Moghaddam described them in a live debate in January 2021.[48] These schemes are not identical, but they rest on similar structures and patterns, described below in a simplified composite form, drawn from explanations in several sources[49] and illustrated in more detail with case studies:

1. Entities within the rogue state, for example, Iranian banks, *rahbar* ('pioneer')[50] companies and exchange houses in Iran, are tasked with facilitating sanctioned international trade – whether exports or imports – for designated domestic sectors or businesses.
2. In this, they rely on existing networks of businesses and agents based overseas who are tasked with setting up front companies and accompanying bank accounts through which to accomplish trade. These overseas networks might be managed by rogue state nationals, others posing as third country nationals, or by actual trusted third country nationals.
3. When the sanctioned state needs to export goods, the front company will sell the designated product or commodity to a buyer, knowingly or otherwise, using falsified documentation. The front company will also engage complicit

46. Nikhilesh De and Danny Nelson, 'US Officials Tie North Korea's "Lazarus" Hackers to $625M Crypto Theft', *CoinDesk*, 14 April 2022, <https://www.coindesk.com/policy/2022/04/14/us-officials-tie-north-korean-hacker-group-to-axies-ronin-exploit/>, accessed 12 December 2022.
47. Choe Sang-Hun and David Yaffe-Bellany, 'How North Korea Used Crypto to Hack its Way Through the Pandemic', *New York Times*, 30 June 2022.
48. Talley, 'Clandestine Finance System Helped Iran Withstand Sanctions Crush, Documents Show'.
49. Karnitschnig, 'Iran Teaches Russia its Tricks on Beating Oil Sanctions'; Brett Sudetic and Omid Shokri, 'Iranian Sanctions Evasion and the Gulf's Complex Oil Trade', Middle East Institute, 11 May 2021, <https://www.mei.edu/publications/iranian-sanctions-evasion-and-gulfs-complex-oil-trade>, accessed 12 December 2022; Talley, 'Clandestine Finance System Helped Iran Withstand Sanctions Crush, Documents Show'; Ian Talley, 'How Iran Tapped International Banks to Keep its Economy Afloat', *Wall Street Journal*, 22 June 2022; US Department of the Treasury Financial Crimes Enforcement Network (FinCEN), 'Advisory on the Iranian Regime's Illicit and Malign Activities and Attempts to Exploit the Financial System', FinCEN Advisory, FIN-2018-A006, 11 October 2018, <https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%20508.pdf>, accessed 12 December 2022; King Mallory, *North Korean Sanctions Evasion Techniques* (Santa Monica, CA: RAND Corporation, 2021), pp. 19–41; Niharika Mandhana and Aruna Viswanath, 'North Korea Built an Alternative Financial System Using a Shadowy Network of Traders', *Wall Street Journal*, 28 December 2018; FinCEN, 'Advisory on North Korea's Use of the International Financial System', FinCEN Advisory, FIN-2017-A008, 2 November 2017, <https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf>, accessed 12 December 2022.
50. *Rahbar* companies are affiliates of the Iranian banks that have been sanctioned.

logistics firms to transport the goods, often using well-known techniques to hide the origin of goods, including changing ship names at sea, transferring goods ship-to-ship with electronic tracking turned off, camouflaging goods with non-designated items, or blending and relabelling commodities such as oil at major transhipment hubs. The funds for the sale will be paid into the front company's bank account.

4. Although some funds might be withdrawn and couriered back to the rogue state, most will be used instead to support import activity. Requests for imports from other designated firms or institutions will be issued to the front company, which will then apply similar techniques to buy and transport goods without revealing their destination, paying for the goods with the funds previously received into its account in receipt of exported items. To ensure that this trade balances, centralised institutions such as the Central Bank of Iran monitor this activity and run ledgers which ensure that countervailing transactions are made domestically to ensure exporters receive compensation for the original sale.

These schemes can vary enormously in their complexity. For states under more limited designation, they can be relatively basic and only used to provide a cut-out for exports; for example, according to 2021 research by civil society group Justice for Myanmar, the US-designated Myanmar Timber Enterprise, the main state-owned exporter of timber in Myanmar, uses a single layer of private and undesignated Myanmar-based companies to sell its goods on to US importers.[51] By comparison, and explored further below, the matrix of companies now being used by Iran to sell oil and related goods to customers in South, Southeast and East Asia is multilayered, with various front companies based in locations such as Turkey, the UAE and Hong Kong being used to hide the connection to Iran, sometimes 'trading' the commodities with each other before dealing with the end customer in South, Southeast or East Asia.[52]

51. Justice for Myanmar, 'US Companies Imported Nearly 1,600 Tonnes of Myanmar Teak, Circumventing Sanctions', 11 January 2022, <https://www.justiceformyanmar.org/stories/us-companies-imported-nearly-1-600-tonnes-of-myanmar-teak-circumventing-sanctions>, accessed 12 December 2022.
52. For example, the operations linked to the Hong Kong-based Iranian oil trading front company Triliance Petrochemical Co. Ltd are complex and apparently involve several layers of 'trading' between front companies. See US Department of the Treasury, 'Treasury Targets International Network Supporting Iran's Petrochemical and Petroleum Industries', 23 January 2020, <https://home.treasury.gov/news/press-releases/sm885>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Sanctions Companies for Enabling the Shipment and Sale of Iranian Petrochemicals', 3 September 2020, <https://home.treasury.gov/news/press-releases/sm1114>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Sanctions Companies Selling, Purchasing, and Enabling Iranian Petrochemical Products', 29 October 2020, <https://home.treasury.gov/news/press-releases/sm1168>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Sanctions Companies for Supporting the Sale of Iranian Petrochemicals', 16 December 2020, <https://home.treasury.gov/news/press-releases/sm1214>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Targets International Network Supporting Iran's Petrochemical and Petroleum Industries', 23 January 2022, <https://home.treasury.gov/news/press-releases/sm885>, accessed 12 December 2022; US Department of the Treasury, 'Treasury

The following three case studies illustrate these forms of clandestine finance activity.

Case Study 1: Iranian Petrochemical Sales

Following the US withdrawal from the JCPOA under the Trump presidency, Iran's intermediary trading networks were revived in response to the reimposition of sanctions by the US. Starting in 2019, OFAC designations on various components of Iran's vast intermediary trading network aimed to forestall the country's efforts to sell its petrochemical products in contravention of US sanctions, mostly to markets in East and South Asia. These OFAC designations are focused on interdicting the networks around two crucial brokerage nodes, Persian Gulf Petrochemical Industries Company (PGPIC) and Triliance Petrochemical Co. Ltd. Once designated, all property and interests in property of these entities subject to US jurisdiction are blocked, and US persons are generally prohibited from engaging in transactions with them. Importantly, furthermore, foreign financial institutions that knowingly facilitate significant transactions for, or persons that provide material or certain other support to, the subjects of these designations risk exposure to sanctions that could sever their own access to the US financial system or block their property and interests in property under US jurisdiction.

- In June 2019, OFAC sanctioned Iran's largest and most profitable petrochemical holding company, PGPIC, and 39 of its subsidiaries and foreign-based sales agents, at the time accounting for 40% of Iran's total petrochemical production capacity and 50% of its petrochemical exports.
- In January 2020, OFAC took action against Triliance Petrochemical Co. Ltd, a broker based in Hong Kong which ordered the transfer of the equivalent of millions of dollars to the National Iranian Oil Company (NIOC) as payment for petroleum products (PPs) delivered to the UAE and China, concealing their Iranian origin. Other companies based in Hong Kong (Sage Energy HK Limited), China (Peakview Industries Co. Limited) and the UAE (Beneathco DMCC) were sanctioned by OFAC for the same reason.

Targets International Sanctions Evasion Network Supporting Iranian Petrochemical Sales', 16 June 2022, <https://home.treasury.gov/news/press-releases/jy0819>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Targets Iranian Oil and Petrochemical Trade Network', 6 July 2022, <https://home.treasury.gov/news/press-releases/jy0851>, accessed 12 December 2022; 'Treasury Targets Companies Supporting Iranian Petrochemical Conglomerate', 1 August 2022, <https://home.treasury.gov/news/press-releases/jy0901>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Targets Financial and Shipping Facilitators of Iranian Petrochemicals and Petroleum Sales', 29 September 2022, <https://home.treasury.gov/news/press-releases/jy0980>, accessed 12 December 2022; US Department of the Treasury, 'Treasury Targets Network Supporting Iranian Petrochemical and Petroleum Sales', 17 November 2022, <https://home.treasury.gov/news/press-releases/jy1115>, accessed 12 December 2022.

- In September 2020, six entities based in the UAE and Hong Kong were designated for supporting Triliance's sanctions evasion efforts by, among other things, acting as the purchaser on behalf of Triliance for hundreds of thousands of metric tonnes of Iranian PPs for onward sale. Other companies were used to settle fees owed by Triliance and to facilitate the shipment and resale of PPs.
- Further Iranian, Chinese and Singaporean companies were sanctioned in October 2020 for similarly supporting Triliance's sanctions evasion by settling, processing and transferring the proceeds of PP sales it had brokered for Iranian producers. Chinese and Emirati companies providing shipping services and conducting financial transactions for Triliance as front companies were sanctioned in December 2020.
- More front companies for Triliance and PGPIC and enabling entities were designated by OFAC in June 2022 (including an Indian national, Mohammad Shaheed Ruknooddin Bhore, who managed multiple Triliance front companies), July, August, September and November 2022, and February and March 2023.
- The latest of these designations, in March 2023, is of particular note. As described by OFAC, 39 entities, 'constituting a significant "shadow banking" network', were sanctioned, representing 'one of several multi-jurisdictional illicit finance systems which grant sanctioned Iranian entities … access to the international financial system and obfuscate their trade with foreign customers'. This and similar networks involving front companies in jurisdictions such as Hong Kong, Singapore and the UAE operate precisely the ledger systems referred to in this paper as CFSs that allow Iran to generate 'the equivalent of tens of billions of dollars annually for the Iranian regime'.

As illustrated in this most recent designation by OFAC, front companies and enabling entities are almost always based in Iran, China, Hong Kong or the UAE, with some further entities based in Singapore, Malaysia and India. Resembling a game of 'whack-a-mole', it would appear that US designations and sanctions action serve to expose small portions of a vast network momentarily, only for the network to adapt and compensate with the formation and use of new companies. That sanctioned entities are all based in just a few countries speaks to the lacklustre approach – and thus high-risk nature – of these countries to taking prudent action against Iran's intermediary trading scheme, even after multiple rounds of OFAC actions targeting companies based in their jurisdictions.

Sources: The White House, ‘President Donald J. Trump is Ending United States Participation in Unacceptable Iran Deal’, 8 May 2018, <https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-ending-united-states-participation-unacceptable-iran-deal/>, accessed 16 March 2023; US Department of the Treasury, ‘Treasury Targets International Network Supporting Iran's Petrochemical and Petroleum Industries’, 23 January 2020; US Department of the Treasury, ‘Treasury Sanctions Iran's Largest Petrochemical Holding Group and Vast Network of Subsidiaries and Sales Agents’, 7 June 2019; US Department of the Treasury, ‘Treasury Sanctions Companies for Enabling the Shipment and Sale of Iranian Petrochemicals’; US Department of the Treasury, ‘Treasury Sanctions Companies Selling, Purchasing, and Enabling Iranian Petrochemical Products’, 29 October 2022; US Department of the Treasury, ‘Treasury Sanctions Companies for Supporting the Sale of Iranian Petrochemicals’; US Department of the Treasury, ‘Treasury Targets International Sanctions Evasion Network Supporting Iranian Petrochemical Sales’; US Department of the Treasury, ‘Treasury Targets Iranian Oil and Petrochemical Trade Network’; US Department of the Treasury, ‘Treasury Targets Companies Supporting Iranian Petrochemical Conglomerate’, 1 August 2022; US Department of the Treasury, ‘Treasury Targets Financial and Shipping Facilitators of Iranian Petrochemicals and Petroleum Sales’, 29 September 2022; US Department of the Treasury, ‘Treasury Targets Network Supporting Iranian Petrochemicals and Petroleum Sales’; US Department of the Treasury, ‘Treasury Sanctions Companies Involved in Production, Sale, and Shipment of Iranian Petrochemicals and Petroleum’, 9 February 2023; US Department of the Treasury, ‘Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime’, 9 March 2023, <https://home.treasury.gov/news/press-releases/jy1330>, accessed 16 March 2023.

Case Study 2: Sitki Ayan/ASB Group

A further example of how front companies in permissive jurisdictions can facilitate sanctions evasion is provided by the case of Sitki Ayan and ASB Group.

A dossier of business contracts and bank documents leaked in late 2022 detail the years-long involvement of a Turkish businessman (and close contact of President Recep Tayyip Erdoğan) and his network of companies in facilitating Iran's sanctioned oil trade and clandestine finance schemes. Accusations made against Sitki Ayan and his Gibraltar-registered holding company ASB Group of Companies were substantiated with an extensive designation from OFAC made hours after the leak, which outlines how Ayan and his business network facilitated and concealed the sale and shipment of oil from NIOC.

Following the reimposition of US sanctions on Iran following Trump's withdrawal from the JCPOA in 2018, ASB found a niche in supporting Iran's re-energised illicit oil enterprise by leasing shipping tankers through its subsidiaries to transport oil from Iran to China. ASB also routed payments through an elaborate network of shell companies and banks in India, Russia and the UAE, which, as payments were denominated in foreign currency (most commonly US dollars), were inevitably settled by international banks such as Commerzbank and J P Morgan, which failed to identify their connection with Iran. Oil shipments to Russia also relied on barter for payment, with sanctions-exempt foodstuffs including wheat and sunflower oil offering camouflage for petroleum product purchases, and leaving Iran with both valuable foreign currency and other scarce consumer goods.

Sources: Politico, *'The Turkish Connection: How Erdoğan's Confidant Helped Iran Finance Terror', 8 December 2022, <https://www. politico.eu/article/sitki-ayan-recep-tayyip-erdogan-terrorism-hezbollah-iran-turkey-lebanon/>, accessed 22 March 2023; US Department of the Treasury, 'Treasury Targets Sanctions Evasion Network Generating Hundreds of Millions of Dollars for Qods Force Oil Sales', 8 December 2022, <https://home.treasury.gov/news/press-releases/jy1151>, accessed 22 March 2023.*

Case Study 3: IRGC/Quds Force and Hizbullah

Alongside the widespread use of front companies in countries offering opaque corporate structures and/or with weak supervisory regimes, the Iranian state also mobilises proxies to facilitate its financial activity, notably the IRGC and its Quds Force. As a parallel security structure to Iran's armed forces, these offer Iran a useful functionality for operating its sanctions evasion regime, particularly where operatives are based outside the country.

In March 2020, OFAC designated several IRGC-controlled front organisations used to hide its money-laundering and illicit revenue-generation activities, including a scheme involving a charitable organisation supposedly dedicated to maintaining Shiite shrines in Iraq, donations to which were redirected to supplement the IRGC's own budget.

In the same way, and emulating a strategy employed by North Korea, Iran's foreign embassies offer useful cover for the illicit movement of funds. *Iran International* reported in January 2023 that the country's embassy in Iraq had been the site of an IRGC-maintained money-laundering operation aiding the repatriation of revenues from Iran's illicit petrochemical product sales. Here, embassy staff receive export revenue in cash from Iraqi currency exchanges and then deposit it into the embassy's accounts, supposedly to fund legitimate embassy operations.

Last, Lebanese Hizbullah, often assumed to be a mere recipient of funds from Iran and an ideologically aligned group, also plays a part in facilitating the CFSs of its host and benefactor. For example, to pay for its imports of Iranian oil, in 2022 Venezuela reportedly shipped gold from Caracas to Tehran using Iran-controlled Mahan Air, with senior Hizbullah officials identified as being involved in easing these shipments, later liquidated in Turkey and other nearby countries.

Sources: OFAC's designation of the Reconstruction Organization of the Holy Shrines in Iraq, in US Department of the Treasury, 'Treasury Designates Vast Network of IRGC-QF Officials and Front Companies in Iraq, Iran', 26 March 2020, <https://home. treasury.gov/news/press-releases/sm957>, accessed 17 March 2023; Daniel Salisbury, 'From Missions to Missiles: North Korea's Diplomats and Sanctions-Busting', RUSI Emerging Insights, November 2022; Iran International, *'Exclusive: IRGC Runs Iran's Money Laundering Network in Iraq', 2 January 2023, <https://www. iranintl. com/en/202301317124>, accessed 9 May 2023; Mojtaba Pourmohsen, 'Iran Smuggling Venezuelan Gold to Finance Hezbollah: Document',* Iran International*, 12 December 2023, <https://www.iranintl.com/en/202212124467>, accessed 17 March 2023.*

As these case studies demonstrate, complex corporate structures and financial engineering have allowed Iran to continue to operate its economy – at times by exploiting large international banks – by developing CFSs that benefit both its economy and proxies operating internationally on behalf of the country.

III. The Russian Response

This chapter considers the Russian context, as the Kremlin seeks ways to evade the tightening Western sanctions imposed in response to its full-scale invasion of Ukraine.

Since the Kremlin's full-scale invasion of Ukraine in February 2022, Western allies have placed a wide range of economic and trade sanctions on Russia to reduce its ability to fund and resource its military machine. These sanctions have targeted financial flows by reducing the Kremlin's access not only to the international financial system but also to sales of goods – such as high-tech chips – needed to restock Russian military supplies. They are also being felt in the ability of Russia to export its oil and other hydrocarbon products, as well as to source Western expertise, such as servicing for its Airbus and Boeing civil airliners.

As a result of these restrictions – and with no sign that President Vladimir Putin intends to reverse his course in Ukraine – Russia is increasingly needing to find new sources to fund its military materiel and resourcing requirements, which is encouraging the Kremlin to gravitate towards those other jurisdictions – notably Iran – that have developed their own responses to Western trade and financial sanctions.

Among these responses, discussions of their experience of de-dollarisation took place during Putin's meeting with Khamenei during the summit between Russia, Iran and Turkey in Tehran on 19 July 2022.[53] A reported statement from the Iranian Supreme Leader emphasised 'long-term cooperation between Iran and Russia as being greatly, deeply beneficial to both countries',[54] marking a clear rapprochement between the countries.

In November 2022, Russian and Iranian leaders met again in Tehran, with a visit from Russian Security Council secretary Nikolai Patrushev, a leading ally of Putin, to Iran's President Ebrahim Raisi to deepen trade and security cooperation.[55] The increasingly closer connections materialised in January 2023 with the reporting of the decision of Iran and Russia to connect their interbank communication and transfer systems to help boost trade and financial transactions, overcoming their ban from SWIFT,[56] a model that Russia could look to replicate

53. Khamenei.ir, 'Dollar Must be Removed from Global Transactions', 19 July 2022, <https://english.khamenei.ir/news/9089/Dollar-must-be-removed-from-global-transactions>, accessed 16 March 2023.
54. *Ibid*.
55. *Reuters*, 'Putin Ally Meets Iran Leader as Moscow Deepens Tehran Ties', 9 November 2022.
56. *Reuters*, 'Iran, Russia Link Banking Systems Amid Western Sanction'.

with other key trading partners to mitigate the SWIFT messaging system restrictions more broadly.

In the latest political move, the deputy foreign ministers of Russia, Turkey, Syria and Iran were scheduled to meet again in Moscow in March 2023,[57] but the meeting will now be held at a later undisclosed date.[58]

In line with these growing political ties, Russia is widely reported to have been sourcing military equipment – notably drones – from Iran as it seeks to overcome the resupply challenges posed by Western sanctions. In response – and demonstrating the seriousness with which Ukraine's allies are treating this growing relationship – Western allies are increasingly targeting Iranian entities with sanctions.

For example:

- On 8 September 2022, OFAC designated Safiran Airport Services, an air transportation service provider, for its involvement in the shipment of Iranian UAVs to Russia for its war against Ukraine. Additionally, OFAC designated Paravar Pars Company, Design and Manufacturing of Aircraft Engines, and Baharestan Kish Company and its managing director, Rehmatollah Heidari, for their involvement in the research, development, production and procurement of Iranian UAVs and UAV components, including the Shahed series of drones, for Iran's IRGC and its Aerospace Force and Navy.[59]
- On 15 November 2022, OFAC designated Shahed Aviation Industries Research Center, the firm responsible for the design and production of Shahed-series UAVs used by Russian forces in Ukraine. OFAC also designated Success Aviation Services FZC and i Jet Global DMCC for facilitating the transfer of Iranian UAVs to Russia. To complement the US State Department's designation of the Wagner Group, OFAC also targeted two individuals for facilitating Wagner's acquisition of UAVs from Iran.[60]
- On 6 January 2023, OFAC designated six executives and board members of US-designated Qods Aviation Industry Company, a key Iranian defence manufacturer responsible for the design and production of UAVs transferred for use in Ukraine, now updated on the Specially Designated Nationals and Blocked Persons List, to include its new alias, Light Airplanes Design and

57. *Reuters*, 'Deputy Formins [Foreign Ministers] of Turkey, Syria, Iran, Russia to Meet Next Week, Cavusoglu Says', 8 March 2023.
58. *Reuters*, 'Meeting of Turkey, Syria, Iran, Russia, Officials Postponed – Turkish Source', 16 March 2023.
59. US Department of the Treasury, 'Treasury Sanctions Iranian Persons Involved in Production of Unmanned Aerial Vehicles and Weapon Shipment to Russia', 8 September 2022, <https://home.treasury.gov/news/press-releases/jy0940>, accessed 13 March 2023.
60. US Department of the Treasury, 'Treasury Targets Actors Involved in Production and Transfer of Iranian Unmanned Aerial Vehicles to Russia for Use in Ukraine', 16 November 2022, <https://home.treasury.gov/news/press-releases/jy1104>, accessed 16 March 2023.

Manufacturing Industries. OFAC also designated the director of Iran's Aerospace Industries Organization, the key organisation responsible for overseeing Iran's ballistic missile programmes.[61]

- On 9 March 2023, OFAC designated a China-based network of five companies and one individual for supporting Iran's UAV procurement efforts to the Iran Aircraft Manufacturing Industrial Company (HESA). HESA has been involved in the production of the Shahed-136 UAV model that Iran has used to attack oil tankers[62] and has also exported to Russia.[63]

While the advancement of financial ties and the sourcing of drones are the most high-profile examples, other connections are also important and growing. For example, unable to have its aircraft serviced in the West, Aeroflot has reported that it is starting to send planes to Iran for servicing;[64] Russia has also been learning lessons from Iran on how to develop a shadow fleet of tankers for transporting oil in circumvention of sanctions.[65]

On top of these clear links between Russia and the provision of Iranian drones, the US Departments of Commerce, Treasury and Justice have also recently provided warning of the methods being adopted by Russia to evade sanctions.[66] This Russian activity reflects the Iranian playbook, with the Tri-Seal Compliance Note observing Russia's 'use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of Specially Designated Nationals and Blocked Persons (SDNs) or parties on the Entity List in transactions, and obscure the true identities of Russian end users' and providing a range of red flags that can be indicative of such activity.[67]

Although the sanctions placed on Russia by allied nations are comprehensive, Russia has agency, and it is already developing measures to circumvent these restrictions to continue to fund and resource its military. Indeed, in the March 2023 Foreign Policy Concept of the Russian Federation, the Kremlin makes no

61. US Department of the Treasury, 'Treasury Sanctions Suppliers of Iranian UAVs Used to Target Ukraine's Civilian Infrastructure', 6 January 2023, <https://home.treasury.gov/news/press-releases/jy1182>, accessed 16 March 2023.
62. Jon Gambrell, 'Drone Hits Israeli-Linked Tanker; Iran Frees 2 Greek Tankers', *Associated Press,* 17 November 2022.
63. US Department of the Treasury, 'Treasury Targets Iran's International UAV Procurement Network', 9 March 2023, <https://home.treasury.gov/news/press-releases/jy1331>, accessed 16 March 2023.
64. *Reuters*, 'Russia's Aeroflot Sends Aircraft for Repair to Iran', 11 April 2023.
65. David Sheppard, Chris Cook and Polina Ivanova, 'Russia Assembles "Shadow Fleet" of Tankers to Help Blunt Oil Sanctions', *Financial Times*; Golvar Motevalli and Marc Champion, 'Iran has Lessons on Grim Survival for Russia Under Sanctions', *Bloomberg*, 11 June 2022.
66. US Department of the Treasury, 'Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls', 2 March 2023, <https://ofac.treasury.gov/media/931471/download?inline>, accessed 9 May 2023.
67. *Ibid*.

secret of its interest in supporting the development of circumvention measures, asserting:

> The abuse by certain states of their dominant position in some spheres intensifies the processes of fragmentation of the global economy and increases disparity in the development of states. New national and trans-border payment systems are becoming widespread, there is a growing interest in new international reserve currencies, and prerequisites for diversifying international economic cooperation mechanisms are being created.[68]

As this paper has reviewed, many of the challenges that sanctions are placing on Russia have been faced previously by other rogue states – notably Iran – that have themselves developed means by which to limit the impact of these restrictions. This experience is inevitably instructive for Russia. Evidence is already emerging of Russia taking lessons from Iran's playbook (for example, its development of a shadow oil tanker fleet); partnering with Iran in financial services and technical expertise that it can no longer source from Western nations; and developing financial and trade structures that obfuscate beneficiaries. If allied nations are to create the impact they wish with their restrictive measures, they will need to study the lessons Russia is likely to draw and ensure they anticipate and restrict the attempted adaptations that follow as a result.

68. Ministry of Foreign Affairs, 'The Concept of the Foreign Policy of the Russian Federation', 31 March 2023, para. 10, <https://russiaeu.ru/en/news/concept-foreign-policy-russian-federation>, accessed 15 April 2023.

IV. Weaknesses in the Financial System Response

As emerges from the previous chapters, the evasion techniques employed by Iran often rely on the use of the formal financial system, which has for decades been required to closely monitor the transactions it facilitates for abuse – including sanctions evasion activity. Yet the formal financial system continues to be associated with sanctions evasion, suggesting that the system and those that supervise it need to consider how they should adapt and work harder and smarter to minimise opportunities for abuse.

The integrity of the global financial system is monitored via the implementation of the standards of the FATF. As a result, in the face of rogue state subterfuge, countries that follow the FATF standards and those that have developed their own unilateral sanctions regimes should have measures in place to detect and prevent sanctions evasion, many of which rely on and are implemented by the private sector.[69]

As the gatekeepers of the financial system under the FATF standards, financial institutions and other obliged entities are required to undertake client due diligence (CDD) when they 'onboard' a client, and periodically thereafter; and to monitor client transactions and report suspicious activity to the authorities. Under national laws, they are also required to ensure that sanctions are not breached, which most businesses do by screening customer names and transactions for the presence of, or connection with, designated entities and individuals.[70]

That is the theory, but these requirements are well known to rogue states and their supporting networks, and thus for many of the techniques discussed in this paper, anti-financial crime and sanctions measures are likely to be irrelevant. The funds being transferred to support a rogue state and its proxies will not enter the financial system (for example, because bulk cash is being used) or, if they do enter it, they will either not be moved through the wider international financial system but be channelled through an institution where measures have already been subverted, in a jurisdiction potentially subject to malign outside

69. FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations', updated March 2022, p. 2, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 13 December 2022.
70. Matthew Redhead, 'Deep Impact? Refocusing the Anti-Money Laundering Model on Evidence and Outcomes', *RUSI Occasional Papers* (October 2019), pp. 5–10.

influences (such as that of Iran over parts of the Iraqi banking system),[71] or else they will be sufficiently disguised such that banks are unable to easily detect the malign connection of the transactions they are processing.

While circumvention opportunities will always exist, and the formal financial sector is not always involved in these schemes, there is certainly room for financial crime and sanctions detection measures to provide more effective barriers with regard to the sorts of intermediary trading schemes detailed in this paper that rogue states are using to avoid sanctions. In the case of Iran, documents provided by sources such as Wiki Iran clearly indicate that funds appear to be moving unchallenged through the international financial system, and through accounts set up and/or held by major financial institutions.[72]

This occurrence indicates that CDD checks are either not properly informed or have been subverted by those tasked with setting up front companies and bank accounts. The potential reasons for failure are numerous and could include malfeasance or negligence on the part of the financial institution, but could just as easily reflect the quality of the malign actors' tradecraft and paperwork, taking advantage of weak supervision and controls in countries that turn a blind eye to the activities of rogue states such as Iran. Furthermore, CFSs are set up precisely to avoid interaction with the formal financial system and thus avoid even the most diligent private sector checks.

Either way, as rogue states have their financial activity increasingly limited, financial institutions and those that monitor and audit their activities, as well as those that control and police the financial system, such as central banks and payment settlement systems, must clearly be more diligent if there is any chance of restricting these CFSs as they develop.

As Western financial institutions seek to raise their game, particular challenges must be overcome. For example, those regulated entities charged with monitoring transactions and screening clients rely on measures to identify unusual patterns that do not match expected account conduct and/or have transactional links to those entities that have already been designated under sanctions regimes.[73] These measures take time to have an effect, however, because the platforms require ongoing streams of data to identify unusual or suspicious patterns, and

71. Qassim Abdul-Zahra and Abby Sewell, 'Targeting Iran, US Tightens Iraq's Dollar Flow, Causing Pain', *AP News*, 2 February 2023, <https://apnews.com/article/united-states-government-iraq-business-0628bad5e4d46315951c90681baba202>, accessed 13 December 2022.
72. Karnitschnig, 'Iran Teaches Russia its Tricks on Beating Oil Sanctions'; Talley, 'Clandestine Finance System Helped Iran Withstand Sanctions Crush, Documents Show'; Talley, 'How Iran Tapped International Banks to Keep its Economy Afloat'.
73. Redhead, 'Deep Impact', pp. 8–9.

even then are far from fool-proof, having a reputation both for generating a high proportion of false positives and missing well-disguised false negatives.[74]

Further difficulties are potentially created by the internal operational 'split' within banks between sanctions screening and transaction monitoring. The identification of a sanctions match will lead to the suspension of a transaction and a report to a national sanctions administrator, but this relies on screening revealing a link to a designated individual or entity. If no such link is identified, transactional activity might be identified separately as unusual or suspicious, but not necessarily sanctions related. The sanctions evasion activity might therefore be filed instead as a suspicious activity/transaction report (SAR or STR, depending on the country) to a national financial intelligence unit (FIU). Whether the potential sanctions-related aspects are identified is uncertain, and likely to depend on the effectiveness of an individual national FIU's data analytics and channels for intelligence sharing with other agencies, including the sanctions administrator. Although the capacity of FIUs will vary between countries, available evidence suggests that the majority of SARs/STRs received by many FIUs, even in the developed world, are not immediately exploited, serving instead as a secondary database for investigations.[75]

These basic weaknesses in the system can be exacerbated further by contextual factors at a national level. Some countries that have become central to sanctions circumvention activity have a weak record of implementing anti-financial crime measures, both in the public and private sectors. The UAE, which has been a primary jurisdiction for the establishment of Iranian front companies and has emerged as a hub for Russian investment and financial activity since the Kremlin's full-scale invasion of Ukraine, was added to the FATF's list of 'Jurisdictions under Increased Monitoring' (so-called 'grey list') in March 2022 for its failure to take effective action against a range of financial crimes, including terrorist financing.[76] Turkey, another common presence in Iranian sanctions circumvention trading schemes,[77] has also been on the FATF grey list since October 2021, under a requirement to address fundamental failings in the policing of its financial system.[78]

---

74. Matthew Redhead, 'The Future of Transaction Monitoring: Better Ways to Detect and Disrupt Financial Crime', SWIFT Institute Working Paper, May 2021, pp. 24–27, <https://swiftinstitute.org/wp-content/uploads/2021/05/SIWP-2020-001-AML-Fraud-Detection_Redhead_FINAL_May2021.pdf>, accessed 13 December 2022.
75. Redhead, 'Deep Impact', p. 16.
76. FATF, 'Jurisdictions under Increased Monitoring', March 2022, <https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-march-2022.html>, accessed 13 December 2022.
77. *Politico*, 'The Turkish Connection'.
78. FATF, 'Jurisdictions under Increased Monitoring – Turkey', October 2021, <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2021.html#turkey>, accessed 4 January 2023.

It is noticeable, moreover, how many front companies in Iranian schemes are based in major Asian trading entrepôts such as Hong Kong,[79] which boast large numbers of small import/export firms.[80] Although this might be a coincidence, it is plausible that these firms are set up in locations where they are much more likely to be able to hide in plain sight. By leveraging these permissive environments, rogue states and their agents can gain access to the international finance system at its weak points, and from there move illicit funds throughout the legitimate system.

79. See, for example, US Treasury Triliance designations discussed in Case Study 1: Iranian Petrochemical Sales.
80. Cherry Yeung, 'Import and Export Trade Industry in Hong Kong', HKDTC Research, 4 November 2022, <https://research.hktdc.com/en/article/MzEzODkxODY0>, accessed 13 December 2022.

Conclusion: Refocusing the System

This paper has sought to illuminate the ways in which rogue states, in particular Iran, develop alternative financial systems to circumvent Western sanctions and how a heavily sanctioned state such as Russia might adopt similar practices. It concludes by assessing how Western governments and their private sectors should strengthen and refocus their responses to confront the development of such CFSs by rogue states.

As the case studies in this paper have demonstrated, rogue state CFSs are consistent in the jurisdictions in which they choose to facilitate their activities. The tools used by the international community to improve national financial crime standards, notably FATF evaluations and (where necessary) greylisting, are clearly insufficient to address this malign activity, designed as they were with criminal finance in mind. As this paper has argued, a much greater focus needs to be placed on strengthening the whole financial system against this abuse, not only relying on the private sector but also involving greater commitment and effort from governments via their control of the financial infrastructure (such as clearing and settlement systems) and the development of new standards (such as expanded financial reporting) designed to address the threat from an expansion of CFSs by rogue states.

The international community's response to illicit finance is built on the FATF and its standards, first developed in 1989 in response to the use of the formal financial system to support the laundering of the proceeds of the narcotics trade between South and North America.[81] Over time, these standards have evolved, but their focus – aside from addressing the implementation of UN sanctions on states engaged in the proliferation of WMDs – has been on identifying and disrupting the proceeds of criminal activity (so-called 'predicate offences'), rather than the activity of rogue states.

Alongside the FATF, sanctions – whether applied on a multilateral basis by the UN or on a bilateral basis by individual states or groups of states – have been a cornerstone of the international community's response to security threats for decades. The success of sanctions in coercing behavioural change is varied. In the case of Iran, some, such as the US Treasury, point to the role sanctions played

81. G7 Research Group, 'Economic Declaration', 16 July 1989, <http://www.g8.utoronto.ca/summit/1989paris/communique/index.html>, accessed 4 January 2023.

in bringing the regime to the negotiation table to agree the 2015 JCPOA;[82] yet Iran, labelled in 2019 by the US State Department as 'the world's worst state sponsor of terrorism', has also been subject to terrorism-related sanctions for nearly 40 years, and has shown no sign of diminishing its funding and resourcing of designated terrorist organisations.[83]

As this paper has reviewed, underpinning the response to sanctions of rogue states such as Iran is the development of complex CFSs that allow states to bypass those traditional financial mechanisms that are dominated by Western nations who seek to coerce changes in behaviour via sanctions.

For many European countries, despite the existence of sanctions regimes for decades, it was not until the Kremlin's full-scale invasion of Ukraine that the reality of sanctions implementation dawned.[84]

And herein lies the contradiction. Most European countries perform well in the evaluations undertaken of their anti-financial crime systems and controls by the FATF; yet their awareness of and engagement with the steps required to secure their financial systems against sanctions evasion contrasts poorly, primarily because they have not felt compelled to focus on sanctions implementation before 2022.[85] This suggests that more specific focus and measures are needed to strengthen the financial system against sanctions evasion activity and related CFSs that go beyond mere FATF compliance.

In light of this need for greater awareness of sanctions evasion activity, the necessity to focus more diligently on sanctions implementation and identify systemic vulnerabilities that allow sanctioned jurisdictions to circumvent economic restrictions to continue funding their malign and threatening activity, including financing designated terrorist groups, this paper presents the following recommendations, focused in particular on European governments.

Recommendations

- **Build on Russia sanctions collaboration**. Western unity on Russia sanctions, together with Asian allies, has been notable since February 2022. While gaps between regimes need to be addressed, commitment to designating entities and restricting relevant Russian economic activity has been strong. Allied

82. US Department of the Treasury, 'The Treasury 2021 Sanctions Review', p. 1.
83. US Department of State, 'Country Reports on Terrorism 2019', <https://www.state.gov/reports/country-reports-on-terrorism-2019/>, accessed 4 January 2023.
84. See, for example, RUSI, 'Euro SIFMANet: European Sanctions and Illicit Finance Monitoring and Analysis Network: Warsaw Report', Conference Report, March 2023, p. 1.
85. See, for example, RUSI, 'Euro SIFMANet: European Sanctions and Illicit Finance Monitoring and Analysis Network: Prague Report', Conference Report, December 2022, p. 4.

nations need to build on this unity to ensure that other rogue states that abuse the financial system are presented with an equally united front to ensure gaps in the responses (notably provided by countries that are well known for their weak compliance with global standards) are not arbitraged by bad actors.

- **Acknowledge the threat posed by parallel financial systems**. As the hegemony of the Western-controlled financial system weakens, Western countries must be alert to the development of parallel financial systems that allow for sanctions circumvention.
- **Educate the private sector**. Driven by the rising awareness of growing Russian attempts to circumvent sanctions, significantly greater effort must be made by Western governments to raise awareness of the sanctions evasion methods and activities of rogue states. Typologies – such as those in the US government Tri-Seal Compliance Note – are not sufficiently specific.[86] Details of sanctions designations must be actively used, along with the provision of other open source case studies, to inform the private sector of the specifics of CFSs.[87]
- **FATF is only part of the solution**. Even where states have received strong reviews from the FATF, they should recognise that FATF-related anti-financial crime responses provide only part of the solution for addressing rogue state activity, as it is a system designed primarily to respond to the proceeds of crime, not the development of CFSs. Although FATF pressure is helpful for raising financial crime standards in general, its sanctions-related focus is narrowly defined and thus fails to address those sanctions regimes that are not based on UNSC resolutions.
- **Review financial infrastructure**. Governments are, for the most part, responsible for key elements of the financial system, such as banking settlement systems (TARGET2 for the Euro area,[88] for example). Although it is unrealistic for these systems to monitor transactions in the way required by commercial banks, greater scrutiny must be applied to the standards of those banks that access these systems. Just as correspondent banks are required to ensure the compliance standards of their client banks, so too should clearing and settlement systems satisfy themselves that those using their services have appropriate controls and policies in place to defend against abuse.
- **Identify sanctions evasion platforms**. This paper has highlighted the way in which platforms such as the ACU could be used to facilitate sanctions evasion. Western governments should ensure they are aware of and securing

86. US Department of the Treasury, 'Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note'.
87. For examples of such work, see the publications of the RUSI Open Source Intelligence and Analysis team, <https://rusi.org/explore-our-research/research-groups/open-source-intelligence-and-analysis#latest-publications>, accessed 9 May 2023.
88. European Central Bank, 'What is TARGET2?', <https://www.ecb.europa.eu/paym/target/target2/html/index.en.html>, accessed 9 May 2023.

against this potential repurposing of such platforms, for example by highlighting these risks to those providing banking and settlement services.

- **Strengthen reporting requirements**. Recognising the growth in sanctions evasion activity, government-mandated private sector reporting requirements (such as those Iran-related reporting requirements policed by the US Securities and Exchange Commission – SEC[89]) must be updated to reflect the greater risk of abuse from rogue states. For example, following the lead of the SEC, European regulators should introduce specific reporting requirements related to 'high-risk' countries such as Russia and Iran.
- **Review competency of EU member state sanctions architecture**. As research has identified, sanctions implementation capabilities across Europe vary considerably.[90] The EU should apply greater scrutiny to and auditing of these capabilities and consider the introduction of an EU-level authority responsible for ensuring harmonisation and high standards of EU sanctions implementation.
- **Empower the private sector and clarify responsibilities**. For many in the private sector, sanctions are a compliance challenge. But as frontline actors, the private sector, particularly large globally operating banks, have a central role to play in ensuring compliance of financial systems in lower-capacity countries by using their leverage over these actors to ensure their compliance with financial restrictive measures. Furthermore, as the threat from CFSs rises, clearly private sector responsibility should be apportioned to ensure the right actors are engaged in the challenge of identifying and disrupting this form of emerging sanctions evasion. Too often it is left to the banks to act as the sole element of the financial frontline. Other actors such as auditors should feel equal responsibility to ensure a systemic response to the threat posed by rogue states.

In sum, as rogue states grow in number and have their financial activity increasingly limited, financial institutions and those that monitor and audit their activities, as well as those that control and police the financial system, such as central banks and payment settlement systems, must clearly be more diligent and alert to the threat posed by CFSs. This challenge will grow significantly as allied nations continue to tighten financial and trade restrictions on Russia. Merely relying on the traditional methods designed to respond to the proceeds of crime will not be sufficient to identify and disrupt this activity. New thinking,

89. See new Section 13(r) requirement to report trade with Iran in the Securities Exchange Commission Act 1934, per Section 219 of the Iran Threat Reduction and Syria Human Rights Act 2012, 'Disclosure Pursuant to Section 13r of the Securities Exchange Act of 1934', <https://www.sec.gov/Archives/edgar/data/1310227/000119312519089566/d726291dex993.htm>, accessed 9 May 2023.
90. For an assessment of EU member state sanctions implementation capabilities, see RUSI, European Sanctions and Illicit Finance Monitoring and Analysis Network (Euro SIFMANet), <https://www.rusi.org/explore-our-research/projects/european-sanctions-and-illicit-finance-monitoring-and-analysis-network-euro-sifmanet>, accessed 22 May 2023.

new approaches and new capabilities will be needed if those seeking to secure the financial system against rogue state abuse are to stand a chance.

About the Author

Tom Keatinge is the Director of the Centre for Financial Crime and Security Studies at RUSI.