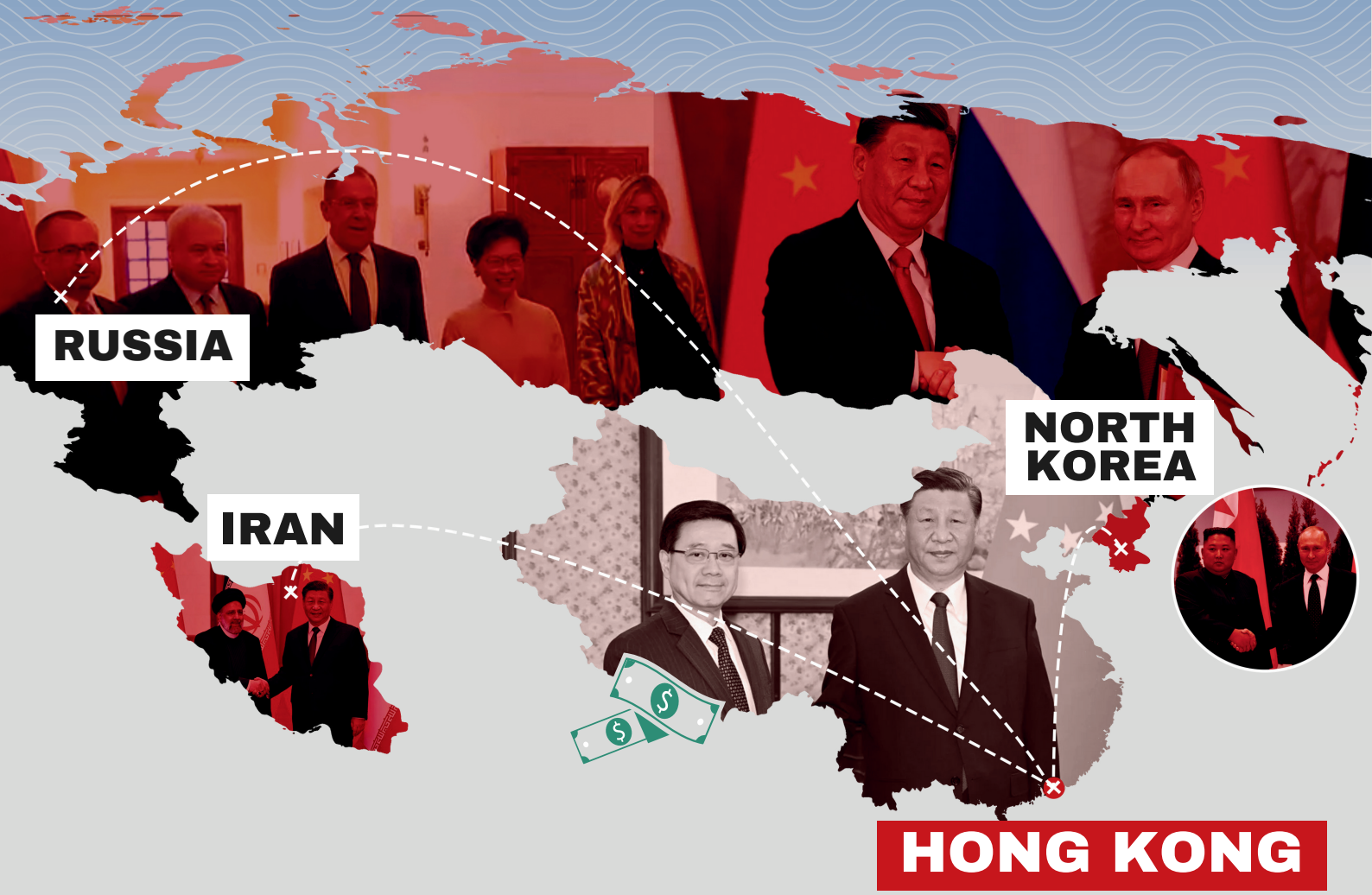
FREEDOM HK
THE COMMITTEE FOR FREEDOM IN HONG KONG FOUNDATION

July 2024
THECFHK.ORG

BENEATH THE HARBOR:

HONG KONG'S LEADING ROLE IN SANCTIONS EVASION



AUTHORED BY SAMUEL BICKETT

About CFHK Foundation

The Committee for Freedom in Hong Kong Foundation (CFHK Foundation) fights for Hong Kong and its people as China continues its crackdown on the city's freedoms. The CFHK Foundation defends political prisoners, free media, and Hong Kong people's right to live peacefully and freely after the handover to China in 1997. Hong Kong's fate is linked to the preservation of freedom, democracy, and international law in the region and around the world.

The Committee for Freedom in Hong Kong Foundation
1100 13th Street NW, Suite 800
Washington, DC 20005

For more information, please visit thecfhk.org.

About the Author

Samuel Bickett is a U.S. lawyer, policy advocate and researcher who specializes in Hong Kong rule of law, human rights, economic sanctions and corporate accountability. He is based in Washington, D.C., where he works closely with the Hong Kong diaspora to advocate for Hongkongers' democratic rights and civil liberties. He is the convenor of the U.S. Hong Kong Policy Roundtable, a collaboration forum for Hong Kong advocacy organizations.

Previously, Samuel lived in Hong Kong and worked as a corporate sanctions and corruption lawyer from 2013 to 2016, studied Mandarin Chinese in Taiwan from 2016 to 2019, and returned to work in Hong Kong from 2019 to 2022.

Disclaimer

This document has been prepared by the Committee for Freedom in Hong Kong Foundation ("we" or "us") for informational purposes only. While all reasonable care has been taken by us to ensure the accuracy of materials in this report (the "Materials"), they have been obtained primarily from open sources and we make no representations or warranties of any kind with respect to the contents.

You should not use, reproduce or rely on the Materials for any purpose other than informational purposes. Any reliance you place on the materials is strictly at your own risk. If you intend to use the Materials for any other purpose (including, without limitation, to commence legal proceedings, take steps or decline to take steps with regard to, or otherwise deal with, any named person or entity), you must first undertake and rely on your own independent research to verify the Materials.

To the fullest extent permitted by law, we shall not be held liable for any loss or damage of any nature arising from or in connection with the reliance on or use of the Materials by you or any third party.

For this report, we have processed company, entity, and individual names recorded in Russian and Chinese. In some instances, names of companies, entities, and individuals have had to be translated or transliterated. Every effort has been made to ensure accuracy in translation/transliteration, and we do not accept liability for any unintentional errors made in this regard.

Report published in July 2024 in Washington D.C.;
Distributed in Washington D.C. (United States), London (United Kingdom), and online at thecfhk.org.

Cover art and report design by Frances Hui.
Photos (from top left to bottom right) from Government of HKSAR, Ministry of Foreign Affairs of the PRC, Embassy of the PRC in USA, State Council of the PRC, and President of Russia.

Are you reading this report in print? Scan this QR code to view our website where you can read and share the online version of the report, as well as access a secure linik to share any information you have about sanctions evaders discussed in this report.

Table of Contents

Executive Summary

Hong Kong until recently was considered a top-tier global financial center, its influence rivalled only by New York and London. Governed by rule of law, its compliance with international standards made it a trusted partner to the world. But all that has changed. With China's assertion of overall political control, Hong Kong now serves Beijing's priorities, even at the cost of global security. Hong Kong's financial and trade strengths have been co-opted by autocrats; they are now used not to connect the globe for good, but to undermine stability and subvert international laws and norms.

This report examines a critical aspect of this phenomenon: Hong Kong's central role in facilitating the transfer of money and restricted technology to Russia, Iran, and North Korea, three countries that the international community has sanctioned for their destabilizing actions. In the growing alliance between these three countries and China, our investigation shows that in many ways, Hong Kong is the hub and these countries are the spokes. Through detailed analysis and investigation using publicly available data collected by C4ADS,[1] a Washington, D.C.-based global security nonprofit, as well as corporate records and other open-source data, we highlight the indispensable role Hong Kong plays in undermining sanctions and threatening global security and stability. Simply put, Hong Kong has gone rogue, serving some of the world's most brutal regimes and damaging international security interests by smuggling military technology, money, and prohibited commodities through the territory to flout sanctions.

Key Findings

- Despite international sanctions, trade between Hong Kong and sanctioned countries, particularly Russia, North Korea, and Iran, has increased significantly in recent years.
- Hong Kong exports to Russia initially dropped significantly but then almost doubled after the February 2022 renewed invasion of Ukraine.
- Hong Kong companies have shipped billions of dollars of goods to Russia for its war effort; our analysis of data from August-December 2023 alone showed that $750 million of the total $2 billion in Hong Kong's shipments to Moscow comprised goods on the U.S. and E.U.'s list of "Common High Priority Items"—the advanced components most sought by Russia for its war effort.
- Hong Kong Chief Executive John Lee's statement in October 2022 that the territory would not enforce global sanctions on Russia gave a green light to illicit operators to set up shop in the city. Many have done so, from Russian tanker owners to Iranian exporters of drone technology.
- The Hong Kong government's regulatory environment, which provides for easy concealment of corporate ownership and rapid creation and dissolution of companies, has facilitated sanctions evasion.
- The slow and inconsistent enforcement of international sanctions by governments around the world has allowed evaders to adapt and continue their operations with relative impunity.

While some of Hong Kong's sanctions-busting behavior has been previously disclosed, our report reveals, for the first time, a range of previously unknown illicit activity. Highlights of our new findings as laid out in this report include:

- Hong Kong company Piraclinos Limited claims to be a fertilizer and charcoal seller, but customs records show it has shipped millions of dollars' worth of integrated circuits to the sanctioned Russian company VMK. The company's directors and owners frequently change, often listed under names of individuals in Cyprus and Central Asia, masking its true beneficial owners.
- After U.S. sanctions targeted Hong Kong company Arttronix International for reshipping drone parts to Iran, owner Li Jianwang swiftly applied to dissolve the company. Once the dissolution was complete, he re-established operations under a new name, ETS International, illustrating the ease with which sanctions evaders can resume business in Hong Kong. To date, neither Li nor ETS have been targeted for sanctions.
- Two Hong Kong-based companies, HK Shipping Cooperation Limited (HKSC) and HK Petroleum Enterprises Cooperation (HKPEC), sought to facilitate significant oil deals with Iranian oil company Sahara Thunder, including arranging vessels for ship-to-ship transfers and the sale of oil originating from Oman. Both HKSC and HKPEC share the same two shareholders, director, and secretary. Corporate records indicate these companies are part owned by an E.U. citizen and resident, Hungarian Anett Szeplaki.

- Hong Kong consignor Align Trading Co. Ltd. purportedly shipped nearly $2 million of expensive and highly specialized integrated circuits produced by French military technology producer Vectrawave to AO Trek, a Russian company previously alleged by Ukraine to be supplying components for missiles and military aircraft.

- Multiple Hong Kong companies have been involved in the illicit activities of the vessel previously known as *New Konk*, a multiyear saga involving a group of sanctions evaders that used the vessel—under various names—to make illicit ship-to-ship oil transfers with North Korea, create fraudulent ship identities, and launder proceeds using shell companies. The *New Konk* and its series of Hong Kong front company owners have appeared repeatedly in the annual reports of the United Nations Security Council's (UNSC) DPRK Sanctions Committee tracking sanctions evasion, but the ship apparently remains active. Little media focus has been placed on Hong Kong's central role in its movements.

Hong Kong continues to trade on the reputation for adherence to international standards that it built up in the final years of British colonial rule, which ended in 1997, and in the first decade of Chinese control. Most major international financial institutions have significant operations in the city, and until recently its market for initial public offerings (IPOs) regularly bested that of New York City and London. But this reputation no longer reflects reality. Following Xi Jinping's rise to power in 2012, and more forcefully since massive pro-democracy protests in 2019, China has moved to assert near-total political control over Hong Kong, eliminate its democratic institutions, and steadily undermine rule of law. It introduced two national security laws that have seen it imprison political opponents and co-opt the previously independent legal system, while passing several constitutional "reforms" to end free elections and curtail local autonomy.

Hong Kong's emergence as the top global center for illicit finance and trade reflects deliberate government policy. John Lee's October 2022 statement, noted above, that the city would not enforce sanctions on Russia was offered in response to a mega-yacht docked in the city that belonged to a sanctioned Russian oligarch—a particularly visible symbol of the city's embrace of sanctions evaders. And for years, the government has openly flouted its legal obligation to enforce the U.N.'s North Korea sanctions against evaders within its borders. Such failures to act served as a green light for smugglers, making it clear that sanctions will not be enforced.

Because Hong Kong is still seen by many as within the orbit of international order and cooperation, few questions are asked about shipments there. It is simple and cheap to open a Hong Kong-based company and firms in the territory can buy goods produced by U.S. companies like Apple and Texas Instruments with little trouble. Once in Hong Kong, goods can be shipped with no questions asked to countries and companies under Western sanctions and trade controls.

Hong Kong's role in helping Russia continue its assault against Ukraine is startling in its growth and extent. Our analysis of customs data provided by C4ADS shows that following the February 2022 invasion of Ukraine, Hong Kong's semiconductor exports to Russia initially dropped, likely as officials assessed the situation. Yet just eight months after the invasion started—the same month that John Lee said that the territory wouldn't enforce U.S. sanctions—chip shipments had nearly doubled from their pre-war levels. A substantial portion of shipments—nearly 40 percent of goods shipped from August to December 2023, for example—appear on the Common High Priority Items List and are likely fueling Russia's production of military goods such as missiles and aircraft. Many of these shipments consist of goods purportedly made by Western companies such as Intel, Analog Devices, Apple, and Texas Instruments.

Companies based in Hong Kong are also facilitating Iran and North Korea's efforts to trade in military technology as well as oil and other natural resources. These efforts have enabled these countries to buttress their capabilities, prop up their regimes, and obtain much-needed cash.

Hong Kong plays a central role in shipping drone and missile components to Iran, which Iran then provides to Russia and destabilizing militias across the Middle East such as the Houthis. Hong Kong has also played a key role in Iran's use of complex shell company structures to sell its oil illicitly. One such network, known as Triliance, has thus far led the U.S. to target 31 different Hong Kong companies over 10 rounds of sanctions.

For North Korea, Hong Kong acts as a hub for illicit shipping operations by which oil and natural resources are traded to and from North Korea in violation of U.N. sanctions and caps. Often, these transactions are carried out via ship-to-ship transfers at sea using vessels owned by Hong Kong companies. Many of these vessels, like the *New Konk*, regularly use laundered vessel identities and deactivate their transponders to mask their activities.

The Hong Kong government's regulatory environment, which makes it easy to hide the names of corporate owners and allows for the rapid creation and dissolution of companies, has facilitated these evasion activities. Its geography is also crucial: it connects mainland China to the busiest shipping lanes in the world. Its past capitalist, laissez-faire approach to transport and customs reflects its decades as a free port and the absence of taxes on most goods. Huge volumes make it impossible to check everything, even if the government wanted to, which it clearly does not. Because Hong Kong is a major transport

hub, with significant air, shipping, and rail lines that extend to China and from there to Russia, North Korea, and Iran, it is the ideal hub for evading sanctions and transporting materials to these countries.

Efforts to crack down on Hong Kong's sanctions evasion have proved inadequate. In the U.S., it currently takes government authorities months, if not years, to investigate and sanction a company. Yet in Hong Kong, new companies can be set up in a matter of days. There is little to stop sanctions targets from establishing extensive networks of front companies at will, continually creating new avenues for transferring goods and payments. The whack-a-mole strategy of going after individual firms cannot keep up with the ease with the rapid creation and dissolution of companies permitted by Hong Kong regulations. Successfully stemming these activities requires a new and forceful approach.

We recommend the following:

1. The U.S. should use its secondary sanctions authority to designate Hong Kong and Chinese banks financing illicit trade, adding them to the Specially Designated Nationals List and blocking their access to U.S. markets and U.S. dollar clearing. The Biden Administration has repeatedly threatened to do so without acting on these threats. It is time to act.

2. The U.S. should Designate Hong Kong as a Primary Money Laundering Concern ("PMLC"). A PMLC designation would authorize the Treasury Department to pursue special measures against Hong Kong as a jurisdiction (as well as particular financial institutions) to prevent illicit transactions, such as requiring U.S. financial institutions dealing with Hong Kong to disclose the beneficiaries of accounts opened by Hong Kong individuals or companies in the United States as well as the customers of Hong Kong banks using the U.S. financial system to clear dollar transactions. It would effectively act as a "middle-ground" preventive measure, strengthening the U.S. government's tools for enforcement while stopping short of what is now a politically impractical full-fledged sanctions regime against Hong Kong.

3. Congress should act to increase resources and coordination across government departments responsible for sanctions and export control enforcement. This would involve significantly increasing funding for additional resources, including data and analytical tools and personnel, to the Commerce, Treasury, and State Department offices responsible for investigation and enforcement. Additionally, there is a pressing need to formalize and regularize cross-departmental coordination across sanctions and export control investigation and enforcement offices, which to date has often been conducted ad hoc without a centralized coordinating authority.

4. The U.S., E.U., and their allies should focus more resources on targeting individuals as well as the associated entities facilitating sanctions evasion—notably logistics firms, insurers, and corporate registry services providers. By merely sanctioning companies directly engaged in trading illicit goods, Western authorities are attacking the stem without reaching the root. Individuals can set up new companies with ease and avoid sanctions, and they often do so by partnering with the same service providers, which along with financial firms make up the core infrastructure of Hong Kong's sanctions evasion environment.

5. Global financial firms should enhance anti-money laundering (AML) procedures to capture data like customs records and suspicious vessel activity. Banks regularly review and flag public reports on their clients. However, to our knowledge, no financial firm has incorporated technical data such as customs records and suspicious vessel tracking data into these reviews. Banks should enhance their data collection and review capabilities in complying with "know your customer" and AML requirements.

6. The U.S., E.U., and their allies should increase enforcement and penalties against manufacturers and distributors of sensitive technologies. This includes imposing strict civil penalties on companies that knowingly or negligently allow their products to be diverted to sanctioned entities and launching enforcement actions against particularly egregious offenders. Increasing the cost of inaction will get companies to take their compliance obligations seriously.

The world has changed, and the U.S. and the international community have failed to adapt. Hong Kong has become unrecognizable from its prior role as a reliable partner in maintaining international order and stability. The U.S. and the international community must act quickly to adjust to these new circumstances, or else Hong Kong will solidify its role as a key destabilizing force in the world.

Glossary of Frequently Used Terms & Acronyms

Term	Meaning
AIS	Automatic Identification System, a mandatory location transmission device used to track vessel locations.
AML	Anti-Money Laundering, a set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income. AML measures are aimed at detecting and reporting suspicious financial activities, ensuring financial institutions comply with regulations, and preventing the misuse of the financial system for money laundering, terrorist financing, and other illicit activities.
BIS	Bureau of Industry and Security, a U.S. government agency within the Department of Commerce that regulates the export of sensitive goods and technologies to enhance national security and foreign policy objectives.
CCL	Commerce Control List, a list maintained by the Bureau of Industry and Security (BIS) that categorizes items subject to export control regulations under the Export Administration Regulations (EAR). The CCL includes goods, software, and technology that have military, nuclear, or dual-use applications.
CHPL	Common High Priority Items List, a list maintained by the U.S., E.U. and their allies of items that are of the highest priority for Russia in its war effort, such as integrated circuits and other essential technology.
Dual-use item	An item or good with both civilian and military applications. These items are subject to export control regulations because they have the potential to contribute to military capabilities or weapons development while also having legitimate commercial uses.
DU Code	A code used in the E.U. to identify dual-use items that have both civilian and military applications. The DU Code helps in categorizing and controlling the export of these items to prevent their misuse for military purposes or in activities that pose national security risks. E.U. equivalent of a U.S. ECCN.
ECCN	Export Control Classification Number, an alphanumeric code used in the CCL to identify items for export control purposes. The ECCN determines the level of control and licensing requirements needed for exporting a specific item. U.S. equivalent of an E.U. DU Code.
Entity List	A list maintained by BIS that identifies foreign parties, including companies, organizations, and individuals, that are subject to specific license requirements for export and re-export of certain U.S. goods, software, and technology. Entities on this list are believed to be involved in activities contrary to the national security or foreign policy interests of the United States.
Export Controls	Regulatory measures implemented by governments to restrict the export of certain goods, technologies, and services for reasons related to national security, foreign policy, and economic protection. Export controls often involve licensing requirements, prohibitions, and penalties for non-compliance. In contrast to sanctions, which apply to "persons" or countries, export controls apply to goods.
HS Code	Harmonized System Code, an internationally standardized numerical system used to classify traded products. Developed by the World Customs Organization (WCO), HS Codes are used by customs authorities around the world to identify products for the application of tariffs, collection of trade statistics, and enforcement of trade regulations, including sanctions. Each code corresponds to a specific product or category of products.

JCPOA	Joint Comprehensive Plan of Action, an agreement reached in 2015 between Iran and the P5+1 group of countries (China, France, Russia, the United Kingdom, the United States, and Germany) along with the European Union. The JCPOA aimed to ensure that Iran's nuclear program is exclusively peaceful in exchange for the lifting of economic sanctions. In May 2018, the United States unilaterally withdrew from the agreement, leading to the reimposition of U.S. sanctions on Iran.
OFAC	Office of Foreign Assets Control, a U.S. Department of the Treasury agency responsible for administering and enforcing economic and trade sanctions (but not export controls, which are the responsibility of BIS).
PMLC	A designation used by the U.S. Department of the Treasury to identify foreign financial institutions, jurisdictions, or entities that pose significant risks of money laundering. This designation, under Section 311 of the USA PATRIOT Act, allows the Treasury to impose special measures to protect the U.S. financial system from money laundering and other illicit activities associated with the designated entities.
Primary Sanctions	Direct restrictions imposed by a country on its own nationals, entities, and individuals and entities within its jurisdiction. These sanctions apply to U.S. Persons (see definition below).
Sanctions Evasion	The act of deliberately circumventing or violating international sanctions imposed by governments or international bodies. This can involve various tactics such as falsifying documents, using third-party intermediaries, transshipping goods through third countries, and utilizing complex financial networks to obscure the true nature of transactions, thereby enabling sanctioned entities to continue prohibited activities.
Secondary Sanctions	Sanctions imposed by a country that target non-compliant foreign individuals and entities, even if they have no direct connection to the sanctioning country. These sanctions aim to deter third-party countries, businesses, and individuals from engaging in activities with targeted countries, individuals, or entities by threatening penalties such as restricted access to the sanctioning country's financial system or markets.
Transshipment	Shipping goods to an intermediary location before forwarding them to a final destination. This practice is often used to disguise the origin or destination of goods and evade sanctions or trade restrictions.
UNSC	United Nations Security Council, one of the six principal organs of the United Nations, responsible for maintaining international peace and security. The UNSC plays a key role in the implementation and enforcement of UN sanctions, including the establishment of sanction regimes, monitoring compliance, and imposing measures such as asset freezes, travel bans, and arms embargoes.
UNSC Sanctions Committee (on North Korea)	A committee established by the United Nations Security Council to oversee the implementation and enforcement of sanctions related to North Korea. The committee is responsible for monitoring compliance with UNSC resolutions, investigating violations, and recommending measures to strengthen sanctions. The goal of these sanctions is to curtail North Korea's nuclear and ballistic missile programs and to promote peace and security in the region.
UNSO/UNATMO	United Nations Sanctions Ordinance and United Nations (Anti-Terrorism Measures) Ordinance, laws in Hong Kong that implement United Nations Security Council sanctions and provide for their enforcement.
U.S. Persons	A legal term that refers to all individuals and entities subject to U.S. jurisdiction, including U.S. citizens and permanent residents (wherever located), individuals physically present in the United States, and corporations and other entities organized under U.S. laws.

Introduction

April 22, 2023, was a bad day for Li Jianwang. On that day, the Shenzhen-based trader learned that the U.S. government had sanctioned his Hong Kong company, Arttronix International (HK) Ltd., for allegedly shipping Western-made drone parts to Iran. He may have found his company's bank accounts frozen, its credit lines blocked, and its business operations at a standstill.

But Li did not sit idle. Hong Kong Companies Registry documents show that within days, he and his co-owner, Liu Jing, filed to dissolve Arttronix. Once the company was delisted and the attention had died down, Li sprang back into action. He registered a new company, ETS International (HK) Ltd., using a different name for the owner and omitting his passport number as director. The Companies Registry did not record any concerns or red flags, and within days of the new filing, the new company was up and running. Li Jianwang was back in business.

Li's story is not unique. In recent years, Hong Kong has become a global hub for sanctions evasion, particularly for those doing business with Russia, North Korea, and Iran. The city's appeal is clear: as its political ties with the West have frayed, so has its cooperation with Western governments. Hong Kong offers an environment where corporate ownership is easily concealed, shell companies can be created or dissolved swiftly, and the government often turns a blind eye to money laundering. This environment allows traders to outmaneuver Western sanctions repeatedly.

While the U.S. government has acknowledged the problem, action has been slow. Despite a December 2023 executive order granting the authority to sanction banks that are financing Russian sanctions evaders in Hong Kong, the Biden Administration has hesitated to act. It has issued repeated warnings, but no financial firms have been sanctioned. The Treasury Department recently stated that its latest round of sanctions would "ratchet up the risk of secondary sanctions for foreign financial institutions," without specifying how this would happen.[2]

This report aims to shine a light on the many companies and individuals that are evading sanctions from the safety of Hong Kong. We focus on Hong Kong's relationships with three countries: Russia, Iran, and North Korea. For each country, we examine how they use Hong Kong's permissive political and legal atmosphere to bypass global sanctions, sell their goods, and import components for military and weapons programs.

We have accessed extensive data, including customs records, corporate registries, U.N. Security Council records, and vessel automatic identification system ("**AIS**") tracking information. We have used this data to examine specific instances of Hong Kong companies and individuals who are using the city as a base to facilitate sanctions evasion.

However, this report can only expose a fraction of the total cases. Our goal is not to list every sanctions evader—an impossible task—but to highlight the pervasive nature of these practices, the Hong Kong government's complicity through inaction, and the failure of Western governments to adapt. Ultimately, our purpose is to underscore how this extensive evasion concentrated in a single city undermines global security and stability, and how it can be stopped.

In the following sections, we will explore the legal frameworks governing sanctions, provide in-depth analyses of specific cases, and offer recommendations to strengthen enforcement and close loopholes. Our goal is to shed light on these practices and urge timely and effective action from the U.S. and its allies.

Part I: Legal Overview

Relevant Global Sanctions and Export Control Framework

- **This section provides a brief overview of the existing global sanctions and export control framework, focusing on the U.S., E.U., and U.N. programs. Each of these programs plays an important role in shaping global trade and security policies, though the U.S. program has an outsized impact due to the core role of the U.S. financial system in the global economy. The departments and programs discussed in this section will be referenced throughout the report.**

U.S. Sanctions and Export Control Framework[3]

U.S. Export Controls

U.S. export control regulations are administered by the Department of Commerce's Bureau of Industry and Security ("**BIS**"). BIS regulates the export of a wide range of sensitive goods via a complex scheme with varying categories and requirements. The extensive list of regulated items is called the Commerce Control List ("CCL").

Many items subject to the CCL have what's called an Export Control Classification Number ("ECCN"), which includes goods like nuclear materials, certain chemicals, and electronics. If an item has an ECCN, it must be managed in accordance with the specific restrictions for that ECCN. These items are often referred to as dual-use items because they have both commercial and military or proliferation applications. Dual-use items require careful control to prevent their use in activities that might threaten national or international security.

Every exported good under BIS jurisdiction that does not fall into a particular ECCN is designated "EAR99"—the catch-all category. These items generally pose less risk and are less likely to be used in a military or proliferation context but are still subject to certain requirements.

Items under EAR99 can usually be exported without a license, except to embargoed countries, prohibited end users, or for prohibited end uses.

Goods relevant to this report usually have ECCNs. Semiconductors, advanced technologies, metals and raw materials all have ECCNs. There are also goods from EAR99 that are being illegally exported to Russia, but since they tend to be more widely available and of lower risk, it is very difficult to prevent this and often not the best use of enforcement resources.

U.S. Sanctions

U.S. sanctions are administered by several government bodies, primarily the Department of the Treasury's Office of Foreign Asset Control ("**OFAC**").

Primary sanctions prohibit transactions between "**U.S. persons**" (a legal term that includes U.S. Citizens, U.S. entities, and individuals/entities physically located in the U.S. or acting within the U.S.) and sanctioned countries or persons. There are three main types:

1. Comprehensive Sanctions: These are broad-based and prohibit almost all transactions between the U.S. and the sanctioned country. Examples include sanctions against Iran and North Korea.
2. Targeted Sanctions: These focus on specific individuals, entities, or sectors within a country. Examples include sanctions against Russian individuals and companies providing support to the Ukraine invasion.
3. Sectoral Sanctions: These target specific sectors of a country's economy, such as financial services, energy, and defense industries. An example would be the sanctions imposed on Russia's energy sector.

These sanctions also prohibit a U.S. person from "facilitating" a transaction between foreigners that would be prohibited if conducted by a U.S. person. The U.S. government interprets facilitation very broadly to include actions such as approving a transaction by a foreign subsidiary, assisting with planning a transaction, or altering foreign subsidiary policies and procedures to permit illicit transactions.

Primary sanctions can also be applied to non-U.S. persons if they "cause" U.S. persons to violate U.S. sanctions, such as by using a U.S. bank to process illicit transactions.

One limitation of primary sanctions is that they usually don't apply to subsidiaries of U.S. persons, with the exception of the Iran and Cuba sanctions programs. This means that a U.S. company can deal with sanctioned individuals or companies through a subsidiary if it is done without explicit or implicit facilitation by a U.S. person. While this is a significant limitation and can be exploited as a loophole, in practice it is a difficult needle to thread. Since the U.S. government considers a wide range of actions to be "facilitation," including virtually any oversight or approvals of subsidiaries, most U.S. companies apply their sanctions policies to foreign subsidiaries.

Secondary sanctions do not require a U.S. nexus. They may be imposed on non-U.S. persons directly or indirectly engaged in certain transactions, such as doing business with persons or countries sanctioned by the U.S. Currently, the sanctions programs for Russia, Iran, North Korea, Hong Kong, and Syria include secondary sanctions provisions.

Unlike primary sanctions violations, which can result in criminal or civil penalties, secondary sanctions block the person's access to U.S. markets and, by extension, much of the global financial system.

The Entity List: A Newer Hybrid Sanctions/Export Control Tool[4]

Traditionally, OFAC sanctions target people, companies, and countries, while BIS export controls target goods. However, BIS has also developed a list of entities that are subject to restrictions on receiving exports of U.S. goods due to national security concerns. This list, known as the Entity List, was created in 1997 for regulating nuclear proliferation but in recent years has been expanded greatly to include a long list of Chinese companies dealing

in advanced technology or associated with the military, as well as a large and growing list of Russian companies associated with the war in Ukraine or advanced technology.

Entities on the Entity List are subject to specific license requirements for the export, re-export, and in-country transfer of specified items.

Technically, companies on the Entity List can apply for a license to obtain U.S. dual-use goods. However, most entities on the list are subject to either a "presumption of denial" or an outright "policy of denial." Thus, in practice, export or re-export of dual-use goods to these entities is generally prohibited.

The Entity List functions as a hybrid tool, combining elements of both export controls and sanctions to restrict entities that pose risks to U.S. national security and foreign policy interests.

E.U. Sanctions and Export Control Framework

E.U. Export Controls

E.U. export control regulations are governed primarily by the Dual-Use Regulation (Regulation (EU) 2021/821). This regulation sets out the rules for the export, transfer, brokering, and transit of dual-use items, which are goods, software, and technology that can be used for both civilian and military applications. The regulation includes the E.U. Control List, which categorizes dual-use items such as nuclear materials, chemicals, electronics, computers, telecommunications equipment, and information security equipment.[5]

Each controlled item is assigned a dual-use code ("**DU Code**"), akin to the U.S. ECCN system, which determines the specific licensing requirements. Items without a DU Code are generally not subject to export license restrictions, but the E.U. applies "catch-all controls" to prevent the export of items that could contribute to military proliferation or human rights abuses.

The regulation provides for different types of export authorizations:

- **E.U. General Export Authorizations (EUGEAs)**: These allow exports to certain destinations under specific conditions.
- **National General Export Authorizations (NGEAs)**: Issued by member states, these must be consistent with existing EUGEAs.
- **Global Licenses**: Granted to one exporter for multiple items and destinations.
- **Individual Licenses**: Granted to one exporter for one or more dual-use items to a specific end-user

E.U. Sanctions

E.U. sanctions, known as restrictive measures, are adopted as part of the E.U.'s Common Foreign and Security Policy (CFSP). Like U.S. sanctions, these sanctions can target countries, entities, or individuals and typically include travel bans, asset freezes, and trade restrictions. Sanctions are adopted through CFSP decisions, which are implemented by regulations directly applicable in all E.U. member states to ensure uniform application across the bloc.[6]

An important limitation to E.U. sanctions is that CFSP decisions typically must be unanimously adopted by all member states. This can make it difficult to obtain unanimous consent on sanctions measures, especially those affecting nations with which certain member states have closer relations. Member states are responsible for enforcing sanctions, with compliance measures including reporting requirements for financial institutions and companies, and penalties for violations determined by national laws.

U.N. Sanctions Framework

U.N. sanctions are administered primarily by the United Nations Security Council (**"UNSC"**), which is mandated by the U.N. Charter "to maintain international peace and security." To fulfill this mandate, the UNSC can issue various enforcement measures including economic sanctions, arms embargoes, financial penalties and restrictions, and travel bans.[7]

The UNSC consists of 15 members, including five permanent members—China, France, Russia, the United Kingdom, and the United States. Actions by the UNSC require a nine-member supermajority vote in favor, but any of the five permanent members can veto an action. Consequently, U.N. sanctions are generally feasible only against smaller "rogue" nations, as actions against any of the permanent members or their close allies are likely to be vetoed.

Once a sanctions regime is adopted, sanctions designations against "persons"—which, like for U.S. sanctions, is a legal term that includes both entities and individuals—can be proposed by member states, the U.N. Secretary General, or the sanctions committees established by the UNSC to oversee specific sanctions regimes. For a relevant sanctions committee to designate a person, there must be a consensus of all committee members through a five-day no-objection procedure. As veto-wielding UNSC members typically influence the sanctions committees, any permanent member can effectively block a designation.

A Panel of Experts, established by the respective sanctions committee, monitors and reports on the implementation and effectiveness of sanctions regimes. They conduct investigations, gather evidence, and issue reports on efforts to evade sanctions. These reports, which often compile substantial evidence of misconduct and "name and shame" the involved individuals and companies, are important resources for those investigating sanctions evaders. However, the reports are advisory and do not compel the UNSC or member states to act on the findings.[8]

Once sanctions designations are made, enforcement relies on member states to implement the measures domestically through national legislation and enforcement mechanisms. This decentralization of enforcement, inherent in the U.N.'s structure, often complicates effective monitoring and enforcement, particularly when countries are uncooperative.

Therefore, while U.N. sanctions play an important role in pressuring targeted regimes, they are typically insufficient on their own. They are usually supplemented by more robust sanctions programs from the U.S., Europe, or other countries.

Hong Kong Sanctions Compliance Framework

Hong Kong claims it adheres only to U.N. sanctions, not foreign state sanctions, because Western unilateral sanctions—or even the Chinese Unreliable Entity List—have "no legal basis" in the city. However, the actual situation is more complex.

Hong Kong implements U.N. sanctions through the locally enacted U.N. Sanctions Ordinance ("**UNSO**")[9] and the U.N. (Anti-Terrorism Measures) Ordinance ("**UNATMO**"),[10] but only indirectly. According to these laws, Hong Kong is to enforce U.N. sanctions if, and only if, instructed to do so by Mainland China's Ministry of Foreign Affairs.

In practice, Beijing has directed Hong Kong to apply U.N. sanctions, such as those against North Korea, but this report will further explore in the North Korea section the extent to which the city enforces these sanctions.

Sanctions evasion is a criminal offense in Hong Kong and is punishable by imprisonment. Under U.N.SO, regulations may prescribe that a contravention or breach shall be punishable—(a) on summary conviction, by a fine not exceeding $500,000 (U.S.$64,000) and imprisonment for a term not exceeding 2 years; or (b) on conviction on indictment, by an unlimited fine and imprisonment for a term not exceeding 7 years. UNATMO provides for penalties of up to 14 years' imprisonment and a fine of HK$5 million (U.S.$640,000).

Although Hong Kong is not bound by the U.S. and its allies' sanctions separate from those implemented by the U.N., such as the Russia and Iran sanctions regimes, it is likely that most financial institutions in Hong Kong voluntarily comply with them. This compliance is due to their global operations and the need to manage risks associated with the international financial system, particularly the U.S. financial system. This is even the case for U.S. sanctions targeting Hong Kong itself. For instance, when former Hong Kong Chief Executive Carrie Lam was sanctioned, she reported that she had been unable to get a bank account in Hong Kong (even with Chinese banks),[11] and when John Lee launched his campaign for Chief Executive, he was reportedly only accepting campaign contributions in cash.[12]

Overview of Existing Sanctions and Export Controls on Russia, Iran, and North Korea

Current Sanctions and Export Controls on Russia

Before Russia's 2014 invasion of Ukraine's Crimea and Donbas regions, certain U.S. and E.U. export restrictions were already in place against Russian targets for national security and non-proliferation reasons, but there was no focused sanctions program for Russia.

Following the 2014 invasion, the U.S. and E.U. implemented "sectoral sanctions" prohibiting the provision of short-term credit to designated banks and energy companies, while simultaneously imposing targeted sanctions on certain Russian officials.[13] BIS also expanded export restrictions on high technology items and added a number of Russian companies to the Entity List,[14] while the E.U. followed suit with prohibitions on export of arms, dual-use goods with military applications, and certain energy-related equipment and technology.[15] These sanctions were progressively tightened between 2014 and 2022, but remained relatively restrained.[16]

In response to Russia's invasion of Ukraine in 2022, the U.S., E.U. and their allies have vastly expanded their Russia sanctions programs, implementing a series of actions targeting various sectors of the Russian economy, its financial system, key individuals and companies, and technology transfers. These sanctions have included adding Russian elites and officials to the SDN List (effectively cutting them off from the international financial system), freezing Russia's foreign currency reserves, freezing Russian bank assets, restricting sovereign debt transactions and lending, and banning imports of oil, natural gas, gold, diamonds, and other valuable goods from Russia.[17]

On the export control front, the U.S. has restricted export of any items on the Commerce Control List, luxury goods, military end use goods, and other specifically listed sensitive items. It has also added many Russian entities to the Entity List and Denied Persons List, which technically imposes a license requirement but in effect has prohibited export of virtually all items to these entities (both from the CCL and general EAR99 goods). The E.U. has similarly blocked Russian access to a range of E.U. goods and technology, including many dual-use goods, oil, luxury products, oil tankers, and industrial products.[18]

The U.S., E.U., and their partners have issued a "Common High Priority List" (**"CHPL"**) as guidance to exporters. This list includes items that are of the highest priority for Russia in its war effort, such as integrated circuits and other essential technology.[19] Given the importance of these items to the sanctions and export control effort, in this report we have focused much of our investigation on Hong Kong's transshipment of goods from the CHPL.

Until December 2023, the U.S. was primarily sanctioning Russians, Russian entities, and foreign entities involved in illicit re-exports or in facilitating evasion of U.S. sanctions. In December 2023, however, the U.S. issued Executive Order 14114,[20] which permits secondary sanctions on non-U.S. financial institutions working with Russian SDNs, even if they are not directly violating U.S. sanctions, as well as anyone supporting the Russian military-industrial base in any capacity. If used assertively, this EO represents a major escalation as it could permit sanctions against Chinese and Hong Kong financial institutions financing the illicit export of Western technology to Russia.

Ukraine's President Volodymyr Zelensky, Germany's Angela Merkel, France's Emmanuel Macron, and Russia's Vladimir Putin meet in December 2019 for negotiations over Ukraine.

Current Sanctions and Export Controls on Iran

Prior to 2015, Iran was subject to stringent multilateral sanctions designed to pressure it to give up its nuclear weapons program. These included U.N., U.S., and E.U. direct sanctions, as well as U.S. secondary sanctions designed to target non-U.S. persons who conducted otherwise lawful business with Iran.[21]

In 2015, Iran entered a multilateral agreement—the Joint Comprehensive Plan of Action ("**JCPOA**")—with the U.S. and other countries to lift nuclear proliferation sanctions (though not ballistic missile and other sanctions) in exchange for limiting its nuclear development activities and subjecting its nuclear program to international monitoring. [22] In 2018, the Trump Administration, acting without U.S. allies, withdrew from the JCPOA and unilaterally reimposed U.S. sanctions. Other parties to the JCPOA did not follow suit.[23]

Thus, whereas prior to 2015 the nonproliferation sanctions against Iran were multilateral and international, today they are largely U.S.-driven.[24] The current U.S. sanctions are comprehensive, targeting Iran's energy, financial, military, shipping, construction, mining, textiles, automotive, and manufacturing sectors, along with any entities that transact with these sectors.[25]

Separate from nonproliferation sanctions, however, the E.U. has joined the U.S. in imposing sanctions on Iran related to the provision of drones and missiles to Russia for use in the war in Ukraine. These sanctions target individuals and entities involved in transferring Iran's missiles and drones to Russia and armed militias in the Middle East such as Hezbollah and the Houthis.[26]

Representatives of nations signing the JCPOA, April 2, 2015 (U.S. Department of States).

Current Sanctions and Export Controls on North Korea

U.N. Sanctions and Export Controls

The U.N. has imposed progressively tighter sanctions on North Korea since 2006, when the country conducted its first nuclear weapons test. These sanctions include bans on trade in military supplies, luxury goods, money transfers, metals, crude oil and petroleum above 500,000 barrels per years, textiles, machinery, and other areas.[27]

Perhaps surprisingly given the world's significant focus on North Korea's nuclear proliferation over the past two decades, the U.N. sanctions list is relatively short, containing only 80 individuals and 75 entities (155 total).[28] This is due to two important factors that limit the impact of U.N. sanctions. First, the sanctions have typically targeted North Korean persons and entities controlled by North Korean persons, but rarely foreign sanctions evaders. Seventy-nine of the 80 individuals on the list are North Korean citizens; the sole foreigner is Taiwanese and is listed without nationality due to the U.N.'s lack of recognition for Taiwan. Second, U.N. sanctions lists must be approved by consensus of the North Korea Sanctions Committee, which effectively allows any of the five permanent members of the UNSC to veto new sanctions targets, including China and Russia. Given these countries' close relationship with North Korea, particularly China, it has been difficult to add new North Korean companies and individuals to the sanctions list over time.

The UNSC thus focuses on naming-and-shaming tactics to try to compel member states to enforce the sanctions. Through 2024, the UNSC Sanctions Committee on North Korea (the "**UNSC Sanctions Committee"**) has published annual and six-monthly interim reports with extensive findings on sanctions evaders.[29] These reports contain detailed information on the foreign companies, vessels, and individuals involved in illicit trade with North Korea. However, in

March 2024, Russia vetoed a resolution to extend the mandate for these reports—a significant blow to the already weakened U.N. sanctions regime on North Korea.[30]

U.S., E.U., and Allied Sanctions and Export Controls

The United States maintains a comprehensive sanctions regime against North Korea, designed to pressure the country into abandoning its nuclear and missile programs, improving its human rights record, and ceasing other destabilizing activities. These sanctions encompass a wide range of measures, including primary sanctions directly targeting North Korean entities and individuals and secondary sanctions aimed at foreign entities engaging with North Korea.

Primary sanctions include strict prohibitions on financial transactions with North Korea, which restrict U.S. financial institutions from dealing with North Korean banks or entities. These measures also involve freezing the assets of designated individuals and entities involved in proliferation activities. Trade restrictions are extensive, banning the export of goods, services, and technology to North Korea, which notably includes luxury goods intended to target the regime's elite.[31]

Secondary sanctions extend the reach of U.S. restrictions by targeting foreign companies and individuals that engage in significant trade with North Korea. This includes entities in China and Russia. The U.S. also sanctions foreign shipping companies and vessels involved in illicit ship-to-ship transfers and smuggling activities to and from North Korea. Cyber activities are also a significant focus, with sanctions imposed on North Korean entities and individuals involved in cyberattacks, such as the Sony Pictures hack in 2014 and the WannaCry ransomware attack in 2017. These sanctions aim to curb North Korea's cyber warfare capabilities and prevent further cyberattacks.[32]

In addition to targeting nuclear and missile programs, U.S. sanctions also address human rights abuses. The U.S. has sanctioned North Korean officials and entities responsible for forced labor camps, extrajudicial killings, and restrictions on freedom of expression and movement. Entities involved in censorship and media control are also targeted, aiming to restrict the regime's ability to control information and suppress dissent.

The European Union (E.U.) has implemented several rounds of sanctions against North Korea, often in concert with U.N. and U.S. sanctions. These measures include import and export bans on coal, iron, seafood, textiles, and other key commodities from North Korea, and prohibiting the export of luxury goods, machinery, and other items to the country. Financial sanctions involve freezing the assets of individuals and entities involved in North Korea's nuclear and missile programs and restricting financial transactions with North Korean banks.[33]

Several other countries, including Australia, Japan, and South Korea, have imposed their own unilateral sanctions on North Korea. Japan bans all trade with North Korea and imposes strict controls on the transfer of goods and technology that could support North Korea's military programs, along with sanctioning entities and individuals involved in weapons development. South Korea has a dual approach of sanctions and engagement, imposing sanctions like those of the U.S. and Japan while also engaging in humanitarian assistance and seeking diplomatic solutions to the North Korean threat.[34]

Part II:
Hong Kong's Role in Sanctions Evasion—Findings and Analysis

Russia

Russian Efforts to Evade Sanctions — Overview

Russia has been open about its efforts to evade sanctions imposed in response to its 2014 and 2022 invasions of Ukraine. It has expanded and formalized its trade relationships with authoritarian countries across the world including China,[35] Iran,[36] and North Korea,[37] as well as some democracies such as India that have remained neutral in the Ukraine conflict.[38]

Shortly after the February 2022 invasion, Russia's imports dropped significantly, but by September they had rebounded to exceed prewar levels. A January 2023 report from the Silverado Policy Accelerator, a U.S. think tank, examined Russian import data to understand the causes of this rebound. They found that as of October 2022, year-on-year imports from the E.U., U.S., and U.K. had declined 52 percent, 85 percent, and 89 percent, respectively. But China, Belarus, Turkey, Kazakhstan, Kyrgyzstan, Armenia, and Uzbekistan imports had increased well beyond their prewar levels, while exports from many other countries had rebounded from their Spring 2022 lows.[39]

Despite strict export controls, Russia has managed to obtain advanced technology from the U.S., Europe, Japan, Taiwan and other countries that have imposed sanctions. In an August 2022 report, the Royal United Services Institute (RUSI), a UK defense think tank, examined extensive data on disassembled Russian weapons found in Ukraine in the first several months of the 2022 invasion. The investigation found at least 450 different unique types of foreign-made components across 27 of Russia's most modern military systems including cruise missiles, Unmanned Aerial Vehicles (drones), and tanks.[40]

RUSI found that 318 of the components —more than 70 percent—originated in the U.S. Of these, at least 80 different types of components were subject to export controls, many of which were in place well before the 2022 invasion, suggesting longstanding evasion of U.S. export controls. Another 77 components were designed and produced by companies from Asia, including Japan and Taiwan, while 55 components came from Europe. Eighty-one of the components were listed on the BIS Commerce Control List. A full 25 percent of the UAV components were manufactured by two U.S. companies: Analog Devices and Texas Instruments. Other U.S. manufacturers identified by RUSI included Intel, Atmel, Cypress Semiconductors, and Microchip Technology.

These goods have reached Russia via transshipment hubs–jurisdictions not subject to sanctions which import restricted goods and re-export them to sanctioned parties. Western manufacturers of these technologies appear to have done little to increase screening of customers to track transshipments. These corporate due diligence failures became so alarming that in March 2023, the U.S. Departments of Commerce, Treasury, and Justice released a joint compliance note to inform and warn manufacturers about Russia's "use of third-party intermediaries or transshipment points to circumvent restrictions, disguise the involvement of [sanctioned individuals or entities], and obscure the true identities of Russian end users." After advising companies to be more vigilant in detecting red flags for transshipment risk came a warning: "Businesses of all stripes should act responsibly by implementing rigorous compliance controls, or they or their business partners risk being the targets of regulatory action, administrative enforcement action, or criminal investigation."[41]

Hong Kong's Role in Russia Sanctions Evasion

Hong Kong, despite its small size, has been a key hub for Russian transshipments of prohibited Western goods, with semiconductor shipments leading the way. The city's exports to Russia have drastically increased since the February 2022 Ukraine invasion. In 2022, as U.S. and E.U. shipments plummeted, Hong Kong's semiconductor exports alone doubled to $400 million, just behind mainland China and far above any other country.[42] According to Russian customs data first reported by Nikkei, 75 percent of semiconductors imported into Russia from February 2024 to December 31, 2022, came from Hong Kong or mainland China. These shipments were valued at $570 million—a more than tenfold increase from the same period in 2021.[43]

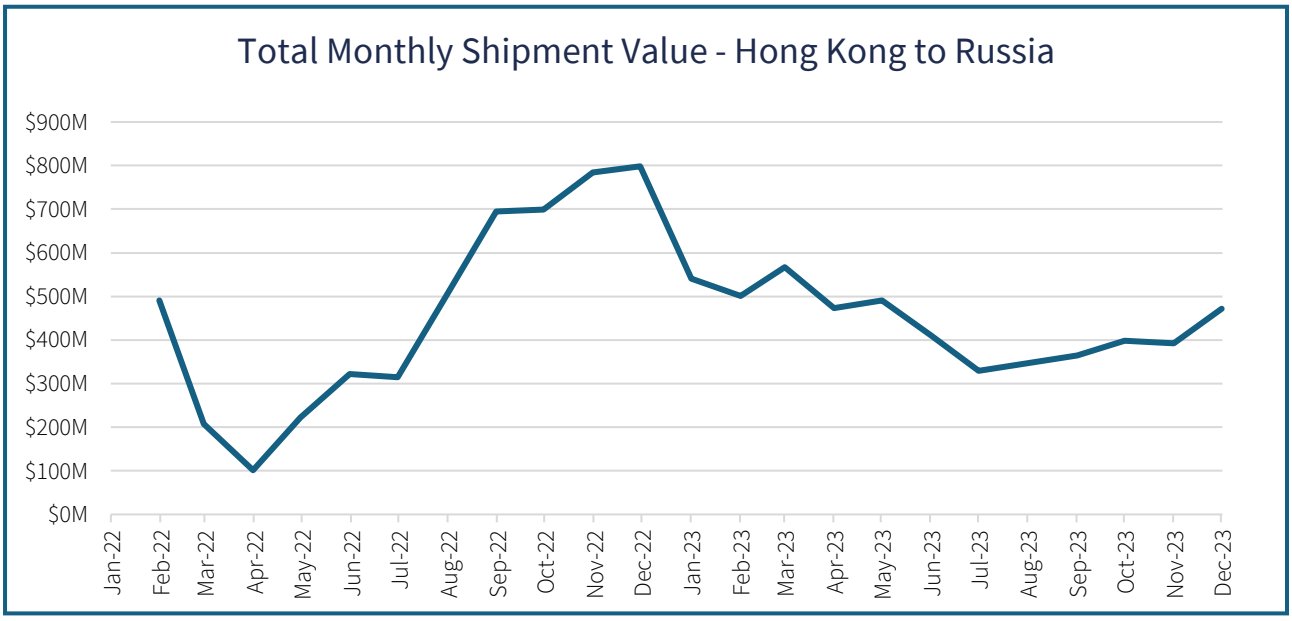
Even before Russia's 2014 invasion of Crimea, Russia's military industry was making use of Hong Kong's corporate secrecy and liberal regulatory environment. The Russian paramilitary group Wagner, which played a major role in the initial stages of the 2022 invasion before its leader Yevgeny Prigozhin rebelled against Vladimir Putin, was established in 2012 in Hong Kong as the Slavonic Corps before changing its name to Wagner in 2013.[44]

These early ties became far more extensive after U.S. and E.U. sanctions in 2022 further limited Russian access to Western markets. According to publicly available data collected by C4ADS, after the February 24, 2022, invasion, Hong Kong and Beijing at first appeared to be restricting exports to Russia. Russian customs data for February showed $490 million in imports originating from Hong Kong, but that number plummeted in March, reaching a low of just $101 million in April.

There was a sudden shift over the spring and summer, however. Russia's imports from Hong Kong began to rise again in May. By August, these imports had surpassed their pre-war value, and by December 2022 the value had reached almost $800 million—62 percent higher than before the war.

Data accessed by the *Wall Street Journal* showed a similar effect for high priority technology critical to the war effort. Just after the invasion in February 2022, Hong Kong's shipments of processors and controllers—key technology for the military—dropped to a trickle, reaching a low of just $150,000 in July 2022. The next month, however, shipments of these components skyrocketed, reaching more than $25 million in October 2022—well above pre-war volumes.[45]

This trade relationship continued in 2023, with Hong Kong solidifying its role as the key hub for transshipment of prohibited U.S. and European goods to Russia. In December 2023, Bloomberg and C4ADS released a new analysis of Russian customs data showing that in the first half of 2023, almost 61,000 cargoes of U.S. and E.U. semiconductors were shipped from Hong Kong to more than 500 Russian companies, more than anywhere else in the world.[46]



**2022 data is from ExportGenius while 2023 data is from C4ADS. There may be minor variations in the data sources due to collection methodology or other reasons.*

Previously Reported Instances of Hong Kong's Links to Russian Sanctions Evasion

Since 2022, a variety of reports on Russian sanctions evasion have implicated Hong Kong companies.

Alexey Mordashov Yacht

In October 2022, in a particularly visible and widely reported incident, the *Nord,* a yacht belonging to sanctioned oligarch Alexey Mordashov, was seen in Hong Kong. In response to questions, Chief Executive John Lee reportedly declined to act, stating that Hong Kong was under no obligation to enforce unilateral sanctions with respect to the yacht.[47] Later that month, the yacht left the city, but apparently on its own volition.[48]

The Nord, Alexey Mordashov's yacht.

Pixel Devices

In December 2022, in a report examining Russia's acquisition of Western components for its Orlan-10 drone, RUSI and Reuters reported that a Hong Kong company, Pixel Devices Ltd., had shipped at least $210 million in electronics to Russia from April through October 2022. Among these shipments, $50 million worth of goods—almost one-fourth—were reportedly manufactured by two U.S. companies, Intel and AMD.[49] These companies produce advanced semiconductors highly sought after by the Russian military, including high-performance CPUs and GPUs. While Pixel Devices told Reuters that they do not sell to defense companies, the report noted that Pixel's website says that they sell to "businesses in diversified sectors including military and aerospace."[50]

RUSI and Reuters reported that the company was originally controlled by a Russian resident of Hong Kong, Kirill Nosov, who told Reuters that he "helped set up the firm but doesn't work for it."[51] At the time of the report, the only current director was Pere Roura Cano, a Spaniard who lives in Catalonia. He told Reuters, "I'm beginning with these people and I'm not

sure what goods are moving." A Reuters journalist who visited the registered office of Pixel Devices in Hong Kong found a small room with cardboard boxes stacked to the ceiling, and no employees.

Asia Pacific Links/SMT-iLogic3

The same RUSI/Reuters investigation found that parts for the Orlan-10 drone were likely being imported by a Russian company, SMT-iLogic3, whose largest supplier by far, reportedly accounting for 25% of its 2022 imports, was Asia Pacific Links Limited, a Hong Kong company controlled by Russian national Anton Trofimov. [52] From February to October 2022, Asia Pacific Links shipped $9 million in components to SMT-iLogic3 and another sanctioned Russian company called Device Consulting, a significant increase from before the war.[53]

Many of these shipments appear to have contained key components for the Orlan-10 UAV, such as quad-band cellular modules that were found in wrecked Orlan-10s, along with GNSS modules made by Swiss company u-blox and computer-on-modules made by American company Gumstix.[54]

In 2023, the Free Russia Foundation further analyzed the SMT-iLogic3 import data and found that Hong Kong was the company's single largest source of semiconductor and integrated circuits in 2022, with China close behind. Overall, FRF found that in 2022 Russia had imported $1.617 million in drones and drone components from Hong Kong and $3.280 million from China.[55]

Agu Information Technology and DEXP International

In April 2023, Nikkei reported that from September to December 2022, a Hong Kong company called Agu Information Technology Co. Ltd. sent Russian wholesaler Mistral more than 60,000 Intel semiconductors worth $18.7 million, with some individual components valued at as much as $13,000 each. Agu was established shortly after Russia's renewed invasion of Ukraine in February 2022. When Nikkei reporters visited Agu's head office address, they found an apartment complex with corporate offices on lower floors, but no sign of Agu on the door plates.[56] On its website, Agu claimed it acquired components directly from manufacturers including Intel and Samsung, but Intel claimed to have no record of any transactions with Agu.[57]

Nikkei also revealed shipments by another Hong Kong company, DEXP International Limited, which in October and November 2022 shipped $2.5 million in Intel and AMD semiconductors to Russian electronics wholesaler Atlas, which appears to be operationally commingled with a larger electronics retailer, DNS Group. From the invasion in February 2022 through December 2022, according to customs data reviewed by Nikkei, Atlas imported at least $49 million in semiconductors.[58]

Significant trade in Texas Instruments and Analog Devices chips

In December 2023, using data and analysis provided by C4ADS, Bloomberg reported the prominent role that semiconductors manufactured by Texas Instruments and Analog Devices—both U.S. companies—played in the illicit Hong Kong to Russia trade. Reviewing data from January to May 2023, the report found that over 200 businesses in Russia received 17,000 TI chips worth $25 million, with $5.3 million in chips sent to two sanctioned companies, NPP Itelma and VMK. As for Analog Devices, customs records showed 13,000 chips shipped to two sanctioned Russian companies during the same period.[59]

Both TI and Analog Devices claimed that they had suspended shipments to Russia after the invasion and that any reshipments were unauthorized. They did not, however, indicate that they have any measures in place to audit their resellers for illicit shipments or otherwise trace their products' movements.

U.S. Sanctions Evasion Prosecutions Involving Hong Kong

While criminal charges for evading sanctions against Russia have been fairly rare, particularly given the extensive nature of these violations, in at least two cases the U.S. Department of Justice has charged defendants with Hong Kong links.

U.S. v. Maxim Marchenko

In September 2023, Russian national and Hong Kong resident Maxim Marchenko was arrested and charged with conspiring to defraud the United States, smuggling, wire fraud, and money laundering for purchasing U.S. dual use goods and transshipping them through Hong Kong to Russia. Marchenko allegedly operated several Hong Kong companies: Alice Components Ltd., Neway Technologies Ltd., and RG Solutions Ltd. [60] Through these companies, he allegedly transshipped dual use electronics from New York-based eMagin, the only manufacturer of micro-OLEDs in the U.S.,[61] to Russia-based Infotechnika, an electronics seller. Infotechnika shared its address with NPO Electronic Systems, a Russian electronics reseller, and its phone/IP address with another entity, NPC Topaz. NPO was added to the Entity List in March 2022.

The mini-OLEDs made by eMagin have important military uses in rifle scopes and similar equipment. As Marchenko's orders continued to increase, eMagin apparently became skeptical of his purpose and began to question him on his end user. Eventually, suspicious of the responses, they informed law enforcement.[62]

In February 2024, Marchenko pled guilty to one count of money laundering and one count of smuggling. On July 17, 2024, he was sentenced to three years in prison.[63]

U.S. v. Ilya Kahn

In January 2024, Ilya Kahn, a Brooklyn resident who is a triple citizen of the U.S., Israel and Russia, was arrested in Los Angeles and charged with conspiracy to violate the Export Control Reform Act for exporting dual-use technology to Russian state-connected company ELVEES, which was sanctioned in March 2022.[64]

Kahn ran two companies in the U.S.: Senesys Inc. in California and the Sensor Design Association in New York. The prosecution alleges that through these companies, in February and March 2022 he exported U.S.-made microcontrollers to ELVEES through intermediaries including an unnamed "Hong Kong-based shipping company."[65]

It is unclear from the criminal Complaint which Hong Kong shipping company was involved (The U.S. Department of Justice does not typically name unindicted co-conspirators). According to trade data collected by C4ADS, ELVEES and its full name "Electronic Computer Information Systems" do not appear in the Hong Kong to Russia shipping data for 2022 and 2023.

New findings and Analysis from Russian Customs Data

Trends in 2023 Common High Priority Items List Sample Data

For this report, we conducted new data analysis of Hong Kong's shipments to Russia with particular focus on items on the CHPL. As noted above, the CHPL was developed by the U.S., E.U., and their Russian sanctions partners. It contains 50 Harmonized System codes ("**HS Codes"**)—goods category designations used in the shipping industry—that consist of goods critical to the development of Russia's military systems used in Ukraine.[66] Many of the most critical items on the list are integrated circuits and other small electronic components, which the Russian military needs to manufacture high-tech weapons and communication systems.

According to data collected by C4ADS, between August 2023 and December 2023, Hong Kong consignors shipped $1.973 billion worth of goods to Russian buyers. Of those shipments, 11 out of the top 25 HS Codes by goods value are items on the CHPL. These 11 CHPL HS codes alone made up 74,318 shipments valued at $750 million—nearly 40 percent of the total value of all goods shipped to Russia during this period. They were led by four categories of semiconductors: data receivers (HS Code 851762), computer processors and controllers (854231), digital storage and input/output units (847150), and "other integrated circuits" (854239). Other CHPL items in the Top 25 shipments included static converters, amplifiers, memory chips, and diodes.

To further assess these shipments, we examined a sample of this vast dataset consisting of all cargoes meeting all the following parameters:

1. Arrived at Russian customs in December 2023;
2. Shipped by Hong Kong companies;
3. Goods listed as manufactured by companies in the U.S., E.U., or Asian democratic allies; and
4. Categorized under the 11 HS Codes on the CHPL listed in the above chart.

(hereafter the **"December 2023 CHPL dataset").** This dataset included 6,489 separate cargoes valued at $63.7 million. The individual cargoes ranged in value from more than $3 million to just 12 cents.

Top 25 HS Codes by Value for Goods Shipped from Hong Kong to Russia, April-December 2023

Total Shipment Value	HS Code	HS Code Description	On US Common High Priority Items List?
$214,492,748.01	851762	Machines for the reception, conversion, and transmission or regeneration of voice, images or other data, including switching and routing apparatus.	Yes
$166,825,303.43	854239	Electronic integrated circuits: Other.	Yes
$143,887,884.13	854231	Electronic integrated circuits: Processors and controllers, whether or not combined with memories, converters, logic circuits, amplifiers, clock and timing circuits, or other circuits.	Yes
$81,704,353.92	847150	Digital processing units other than those of subheadings 8471.41 or 8471.49, whether or not containing in the same housing one or two of the following types of unit: storage units, input units, output units.	Yes
$71,465,598.89	847170	Storage units.	No
$58,727,531.96	847330	Parts and accessories of the machines of heading 8471.	No
$58,500,121.93	847130	Portable automatic data-processing machines, weighing not more than 10 kg, consisting of at least a central processing unit, a keyboard, and a display.	No
$37,311,001.52	851761	Base stations.	No
$27,650,041.46	850440	Static converters.	Yes
$25,152,301.61	847180	Other units of automatic data-processing machines.	Yes
$22,755,868.19	854390	Parts of machines and apparatus of heading 8543.	No
$22,433,759.25	854233	Amplifiers.	Yes
$22,191,467.81	901890	Instruments and appliances used in medical, surgical, dental or veterinary sciences, including scyntigraphic apparatus, other electromedical apparatus and sight-testing instruments; parts and accessories thereof: Other.	No
$21,967,555.37	854129	Transistors, other than photosensitive transistors: With a dissipation rate of less than 1W.	Yes
$21,107,788.70	854232	Memories.	Yes
$20,134,251.19	851779	Other apparatus for the transmission or reception of voice, images or other data, including apparatus for communication in a wired or wireless network.	No
$19,608,194.57	851830	Headphones and earphones, whether or not combined with a microphone, and sets consisting of a microphone and one or more loudspeakers.	No
$13,905,705.02	854110	Diodes, other than photosensitive or light-emitting diodes.	Yes
$13,385,475.00	890120	Tankers.	No
$11,542,826.37	853400	Printed circuits.	Yes
$10,138,830.40	901819	Other electro-diagnostic apparatus (including apparatus for functional exploratory examination or for checking physiological parameters).	No
$9,729,235.75	271019	Petroleum oils and oils obtained from bituminous minerals, other than crude; preparations not elsewhere specified or included, containing by weight 70 % or more of petroleum oils or of oils obtained from bituminous....	No
$8,553,189.60	830990	Other: Stoppers, caps and lids (including crown corks, screw caps and pouring stoppers), capsules for bottles, threaded bungs, bung covers, seals and other packing accessories, and parts thereof, of base metal.	No
$6,793,471.81	853710	Boards, panels, consoles, desks, cabinets and other bases, equipped with two or more apparatus of heading 8535 or 8536, for electric control or the distribution of electricity, excluding switching apparatus of heading 8517.	No
$6,648,817.65	870380	Other vehicles, with only electric motor for propulsion.	No

Analysis of this dataset indicates that the goods were shipped by 206 different Hong Kong companies, known as consignors.[67] Seventeen different consignors sent at least 100 separate cargoes through the month. The top consignors were Xin Quan Electronics Hongkong Co Limited (585 instances), Chipgoo Electronics Limited (348), Ace Electronic HK Co Limited (240), Most Technology Company Limited (222), Msuntech Electronics Group Co Ltd (212) and Analog Technology Limited (203).[68]

The December 2023 CHPL dataset further reveals that the shipped goods were reported to be manufactured by 131 different Western goods producers. Eleven producers were named in more than 100 cargoes: Texas Instruments (1,492 instances), Analog Devices (1,315), Microchip Technology (438), ST Microelectronics (403), ON Semi (343), Maxim (231), Infineon (202), Apple (170), NXP (142), Intel (132), and Vishay (112). All these companies are U.S.-headquartered except STMicroelectronics (Swiss), Infineon (German), and NXP (Dutch).[69]

The list of top goods producers by total value of cargoes reported in this customs data is somewhat different: Intel ($7.26m), Analog Devices ($7.18m), Dell ($4.77m), Apple ($3.90m), Nvidia ($3.52m in 16 cargoes), Xilinx ($3.43m in 83 shipments), Micro-Star International ($2.61m in 4 cargoes), Compound Photonics ($2.03m in 1 shipment), Vectrawave ($1.99m in 2 cargoes).[70] All of these companies are U.S.-headquartered except Micro-Star (Taiwan) and Vectrawave (France).[71]

The reason for the disparity in top goods producers measured by quantity of cargoes and shipments is mainly due to the different nature of the goods. Texas Instruments mass produces cheap semiconductors and other small technology. A company like Vectrawave, on the other hand, produces highly specialized custom chips that can cost thousands of dollars, and many of the top producers by value like Intel and Nvidia tend to produce more expensive products than Texas Instruments.

In the Dec. 2023 CHPL dataset, U.S. semiconductor company Analog Devices appears near the top of the list of manufacturers by both quantity and volume.

Notable Cases within the December 2023 Customs Data

- *Beyond looking at overall trends, we used the December 2023 CHPL dataset to identify and further investigate suspicious shipments, consignors, goods producers, and Russian consignees (recipients). This section will examine some of the more notable of these case studies.*

Case 1

Piraclinos Limited

A "charcoal and fertilizer" seller that shipped millions in integrated circuits to sanctioned company VMK.

On its website, Hong Kong company Piraclinos Ltd advertises itself as a wholesaler with a "wide selection of charcoal and fertilizers with worldwide delivery."[72] Yet in the December 2023 CHPL dataset, it is listed as having shipped over $2.5 million in electronic integrated circuits and other common high priority items to sanctioned Russian company VMK, making it the consignor with the fourth highest value of CHPL goods shipped to Russia that month.

Piraclinos website home page advertising "charcoal and fertilizers"

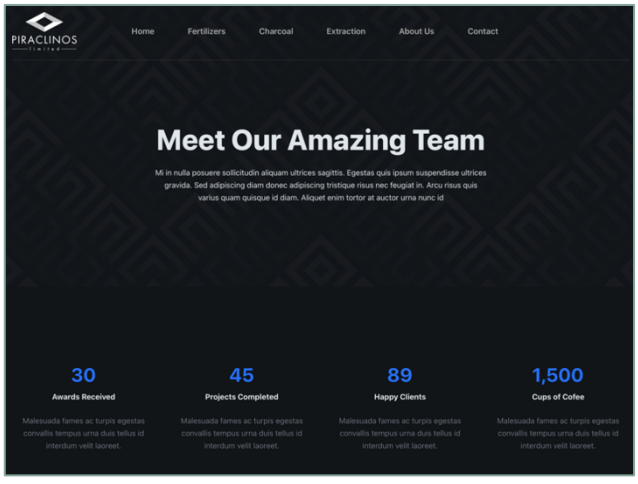
Piraclinos and VMK appear closely tied. In the December 2023 CHPL dataset, Piraclinos shipped CHPL goods only to VMK, and VMK only received Hong Kong-origin CHPL goods from Piraclinos. The U.S. sanctioned VMK in September 2023. OFAC describes VMK as "a supplier of electronic products, including circuit boards, wires, connectors, and microchips," which "supplies electronics to U.S.-designated Joint Stock Company Concern Radio-Electronic Technologies, a subsidiary of Rostec that develops electronic warfare systems for the Russian military."[73]

Beyond the December 2023 CHPL dataset, Russian customs records for 2022 and 2023 collected by C4ADS suggests that this "charcoal and fertilizer" company does little if any real business in these industries. According to this data, the vast majority of Piraclinos cargoes to Russia across this period are listed under HS Code classification 8542 for electronic integrated circuits. There are no reported shipments to Russia under classifications 3101-3105 (fertilizer) or 4402 (charcoal). This does not exclude the possibility that the company sells charcoal and fertilizer to places other than Russia, but the website claim warrants significant skepticism.

In the December 2023 CHPL data, the most valuable Piraclinos cargo by far was one worth $2.03 million consisting of amplifiers—chips used to amplify signals in telecommunications—purportedly from Compound Photonics. Compound Photonics, a.k.a. CP Display, was reportedly an Arizona company that produced tiny micro-LED systems known as LCOS displays, which were small enough to fit on AR glasses to display information on the lenses.[74] The company appears to have been purchased, along with an associated company known as WaveOptics, by Snap Inc., a social media company that also develops and sells AR glasses,[75] around January 2022.[76] While these micro-LED products could have potential military uses, Compound Photonics did not produce amplifiers. Therefore, either the manufacturer or the contents may have been mislabeled either accidentally or deliberately to mask its content.

Other products reportedly shipped by Piraclinos to VMK include semiconductors from a variety of U.S. technology manufacturers, including Cypress Semiconductor, Onsemi, Mini-Circuits Inc., and Dell EMC. Most of these cargoes reportedly weighed very little but had high value, such as a Dell EMC package weighing 0.01 kilogram and valued at more than $11,000. Based on the product descriptions for the cargoes, they appear to be highly specialized electronic components used in telecommunications and signal processing.

The Piraclinos website, aside from advertising fertilizer and charcoal products, contains other red flags suggesting it is not what it claims to be. Pages such as the "About Us" contain nonsensical text, and the website includes only stock photos with no original images nor any details on ownership or employees.[77]



Most of Piraclinos' website consists of nonsense text.

Piraclinos' 2023 Annual Return shows one director, Katerina Hadjikyriacou, and one owner, Svilen Spasov. Both have Cyprus addresses. A post-filing change of director form replaced Hadjikyraicou with Symbat Belekova of Kyrgystan. By 2024, both the owner and director had changed yet again. On the 2024 Annual Return, filed May 3, 2024, the owner was now listed as Demetris Demetriou of Cyprus. Two weeks later on May 20, the company filed a notice that it had changed its director from Belekova to Ahmadkhon Isoev of Tajikistan.

In the case of at least Hadjikyriacou and Spasov, both appear to be financial professionals associated with corporate services firms. A Cyprus resident named Katerina Hadjikyriacou, according to her LinkedIn,[78] is a tax associate at SPL Audit, after having served as a tax consultant at a local Cyprus offshoring firm called Treppides—the job she held during the time someone with her name was director of Piraclinos. According to its website, Treppides is a corporate services firm providing "a holistic range of audit, tax, accounting, legal, consulting and financial advisory services to international companies."[79]

According to the Companies Registry, Hadjikyriacou is a director at 176 different companies in Hong Kong. Most do not appear to have anything to do with Russia trade.[80] All of the above suggests that Hadjikyriacou may be a corporate services professional with little knowledge of, or input into, the companies on which she sits as a director.

Spasov, according to a LinkedIn account by that name,[81] currently lives in Bulgaria (and the name is likely of Bulgarian origin). According to the U.K.'s Companies House, a person by the name of Svilen Spasov has been a director of 13 different U.K. companies,[82] and according to the Cyprus Corporate Registry, Spasov has served as director or secretary of 121 different Cypriot companies.[83] Until February 2024 he worked in the Cyprus office of a business registration services firm called IBFS United, which appears to cater to Russians and to have been founded in Russia.[84] As with Hadjikyriacou, this suggests that Spasov may be a director for hire with little insight or input into the companies to which he is appointed.

Spasov's former company, IBFS United, has made changes to its website in recent months. In an archived version of the website from February 28, 2024, IBFS prominently lists Russia as one of its "company

branches."[85] As of June 14, however, reference to that branch had been removed.[86] (IBFS also lists a Hong Kong branch.)

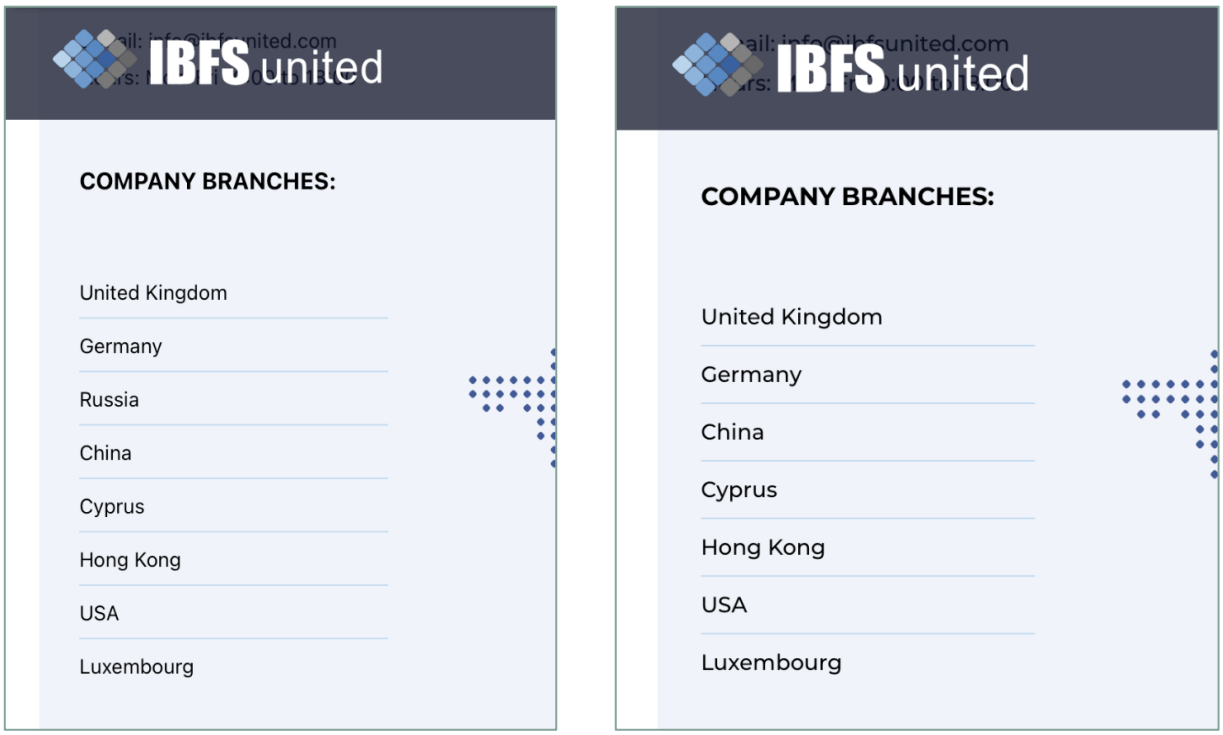
Despite the removal of the Russia office listing, IBFS's ties to Russia remain evident throughout the website. In its Taxation Services section, IBFS notes that it was founded in Russia. And in its Corporate Services section, IBFS repeatedly mentions services it can provide to companies that organize in Cyprus and hold subsidiaries in Russia.[87]

Symbat Belekova, who replaced Hadjikyriacou as Piraclinos' director in 2023, has less of an online presence. According to the Hong Kong Companies Registry, she holds a Kyrgyzstan passport and lists an apartment in Kara Balta, Kyrgyzstan as a registered address.[88] She was the director of a single dissolved U.K. company, Findlay Ink Ltd., where she was listed as Kyrgyz with the occupation of "manager."[89] She holds no other known directorships in Hong Kong, the U.K. or Cyprus.

Demetris Demetriou is a relatively common name in Cyprus, with LinkedIn showing 203 people with this first and last name in the country. In any case, like his predecessors, it is possible, if not likely, that Demetriou is associated with a corporate services firm that provides fronts for companies seeking to hide their beneficial owners.

Ahmadkhon Isoev of Tajikistan also has little online presence using either Western script or common variations on the name in Cyrillic. He holds no other directorships in Hong Kong, the U.K., or Cyprus.

Thus, while it is unknown who on the ground in Hong Kong is really operating Piraclinos, the evidence tends to show that it is little more than a front company, possibly for VMK itself. Our data showed that it shipped high priority goods only to VMK, and VMK received goods only from Piraclinos in the December 2023 data. Its website does not give the appearance of a legitimate company, and the company seems to have gone to great lengths to hide its true ownership.



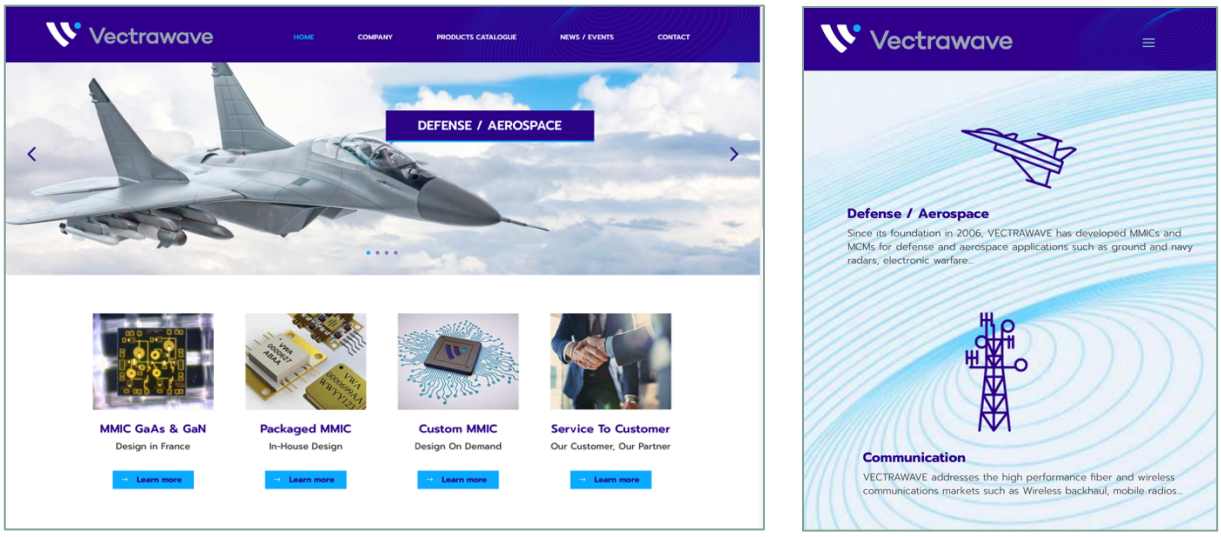
IBFS Website branches section, showing Russia branch in February 2024 (left) and without it in June 2024 (right).

Case 2

Two high-value shipments of Vectrawave integrated circuits

The December 2023 data reveals two notable cargoes of integrated circuits purportedly produced by French company Vectrawave that were reportedly shipped by Hong Kong consignor Align Trading Co Limited to AO Trek, a Russian company that has previously appeared on Ukraine sanctions lists but is not sanctioned by the U.S., E.U., or their allies. The shipments, recorded on December 15 and December 19, are valued at nearly $1 million each but weigh only 8kg and 7kg, respectively.

The goods are described as "monolithic electronic integrated circuits, not for fire automatics, not for military purposes, not for scrap electronic equipment," but these disclaimers may be attempts to mask the real intended use. Vectrawave's main products are highly specialized, advanced semiconductor components, primarily Monolithic Microwave Integrated Circuits (MMICs) that have been custom-made to meet specific requirements for high-tech communication and defense systems.[90] The company's website lists some of the main applications of its products, with "ground and navy radars" and "electronic warfare [systems]" listed first.[91]



Vectrawave's website prominently displays its military and communications specializations.

The Russian recipient of the shipments, AO Trek (АО ТРЭК), has previously been listed as sanctioned by the Ukraine government. The Ukraine government's Sanctions Tracker alleged that Trek is "a Russian supplier of electronic components for missiles and military aircraft," and that it had imported electronic components worth almost $50 million in 2023, all from China and Hong Kong, with rapid increases in deliveries as the year went on.[92] At some point in the first half of 2024, this entry was removed from Ukraine's sanctions database.[93]

Since Vectrawave components are often custom designed for particular functions, repurposing them for different uses is possible but challenging. We cannot verify whether Vectrawave produced these chips directly for a Russian buyer to meet specific defense needs or whether they were produced for another buyer—or even whether the manufacturer is correctly listed on the customs entry. But the description and value of the shipments, the known production focus of Vectrawave, and the involvement of an alleged military supplier in AO Trek raise significant questions about Vectrawave's possible role.[94]

Case 3

Corp-Link International Logistics Ltd.

A Hong Kong shipping company with a niche for illicit Russian goods

As a standalone consignor, Corp-Link International Logistics Ltd is ninth on the list of Hong Kong consignors in the December 2023 CHPL data. Yet this company stands out as unique. In addition to being listed as the consignor for 118 cargoes worth $2.13 million, it also appears on 658 cargoes by 21 other consignors in a "c/o" line—the only such company in the dataset with this apparent dual role. For example, 65 of the 96 December cargoes by Align Trading Co Limited list the consignor as "Align Trading Co Limited c/o Corp-Link International Logistics Ltd."

Over the full 2023 calendar year, data for all shippers indicates that items from the CHPL constituted about 46 percent of all cargoes from Hong Kong to Russia. For Corp-Link, however, 75.6 percent of its 2023 cargoes were from the CHPL.

Of the top 15 HS Codes where Corp-Link is listed as the consignor, 13 are on the CHPL, with integrated circuit HS Codes (8542xx) in the top three spots.

Corp-Link International Logistics Ltd. Cargoes to Russia, Jan-Dec 2023.

	Directly Consigned Cargoes	Directly Consigned Cargoes (CHPL Items)	Cargoes including "C/O Corp-Link"	Cargoes including "C/O Corp-Link" (CHPL Items)
Value (USD)	25,333,267.14	18,897,299.8	5,284,178.80	4,237,168.54
Volume	1,730	895	4,036	3,428

This data suggests that Corp-Link may have developed a niche shipping illicit goods from other consignors, either exclusively as a shipper or in addition to its own work as a seller. Indeed, according to Corp-Link's website, they provide both logistics services and conduct direct trading.[95]

Corp-Link also advertises in Russian on several sites connecting Russian buyers with Chinese suppliers. On one, its description in Russian says, "Corp-Link is a specialized enterprise in international freight transportation, including air and sea transport. It is particularly convenient for handling air freight and has good relationships with airline companies. Our head office is in Hong Kong, with branches in Shenzhen (China) and Taipei. Our guiding principles are a customer-oriented approach and providing professional services for each client."[96]

Unlike many consignors on the list, which often have been recently founded, have a single owner and director, and list a for-hire corporate services company as their secretary and registered address, Corp-Link appears to run a more significant and longstanding operation. According to the Companies Registry, it has been in business since at least 2009.[97] Its 2023 Annual Return lists seven joint owners and directors with varying shareholdings, along with recent transfers from an eighth owner, Kung Suet Fung, who appears to have been bought out in January 2023. [98] The company secretary is not a secretarial services company, but rather one of the owner/directors, Tsoi Kai Tai, and the secretarial address appears to be a private residence in Ma On Shan.[99]

In the December 2023 CHPL dataset, Corp-Link (either as consignor or shipper for other consignors) shipped to five Russian companies: AR-Logistik, Ekspress Import, Ellou Vind, Global Key, and Stroymashkomplekt. Global Key, based in St Petersburg, has been sanctioned by the U.S. for its role in assisting another sanctioned company, Radioavtomatika, "fulfill multiple Russian defense contracts."[100] The other four companies do not yet appear to have been targeted or recommended for sanctions.

Case 4

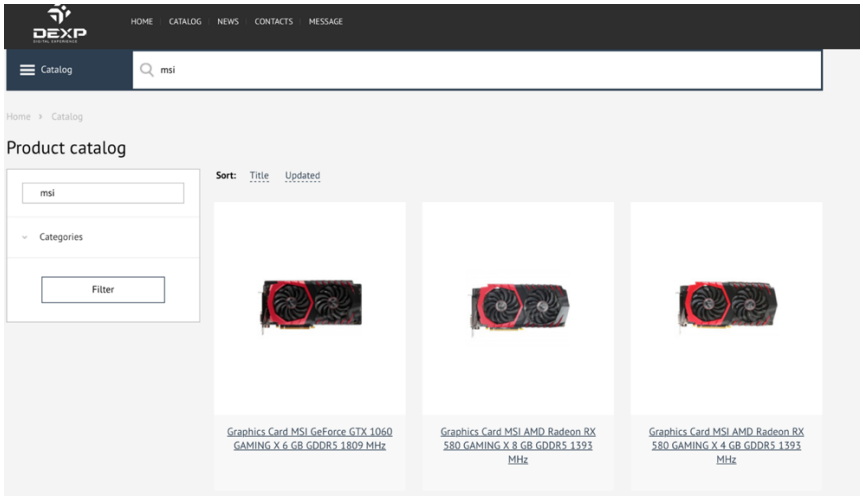
Gleb Khitrin, DEXP, and Stotechno

Shipping advanced GPUs and other high value processors to one under-the-radar Russian company

The highest value Hong Kong consignor in the December 2023 CHPL dataset was DEXP International Limited, with $4.71 million in CHPL goods reportedly shipped to a single Russian company, Vladivostock-based Stotechno (CTOTEXHO). Stotechno was also the highest value consignee in the data. Neither DEXP nor Stotechno have been sanctioned.

The data lists only 17 total cargoes shipped between the two companies, but with high values. Most of the cargoes are six figures, with the highest at $1.23 million. Most are quite heavy, with the largest valued shipment at 3,400 kg (7,495 lbs.), and others weighing in the hundreds of kilograms. The two largest cargoes are listed under HS Code 847180—"other units of automatic data processing machines"—and described in the logs only as "computing devices." The other 15 cargoes are all categorized as microprocessors (854231) or storage devices (847170).

All products are listed as manufactured by MSI (a Taiwanese computer company), Intel, AMD, or Samsung. DEXP maintains a website with a catalog that lists a wide variety of electronic parts, complete appliances, and computers.[101] The only MSI products listed in this catalog matching the 847180 HS Code description are advanced graphical processing units (GPUs, or graphics cards). The GPUs in the catalog are manufactured by U.S. companies Nvidia and AMD, then adapted by MSI for their machines. These devices are expensive and relatively heavy by the standards of computer parts, in line with the high value and weight of the DEXP cargoes.



The DEXP website lists MSI-branded Nvidia GPUs for sale.

Thus, while it is impossible to verify based on the data alone, it is possible that DEXP was shipping GPUs and other higher-end processing units to Stotechno (or full computers with these components inside). GPUs, originally designed for graphics, in recent years have taken on a role as the building blocks of supercomputers and AI data centers due to their advanced capabilities. The most advanced GPUs are designed by American companies Nvidia, AMD, and Intel, and produced in "fabs" in places like Taiwan and the United States.[102]

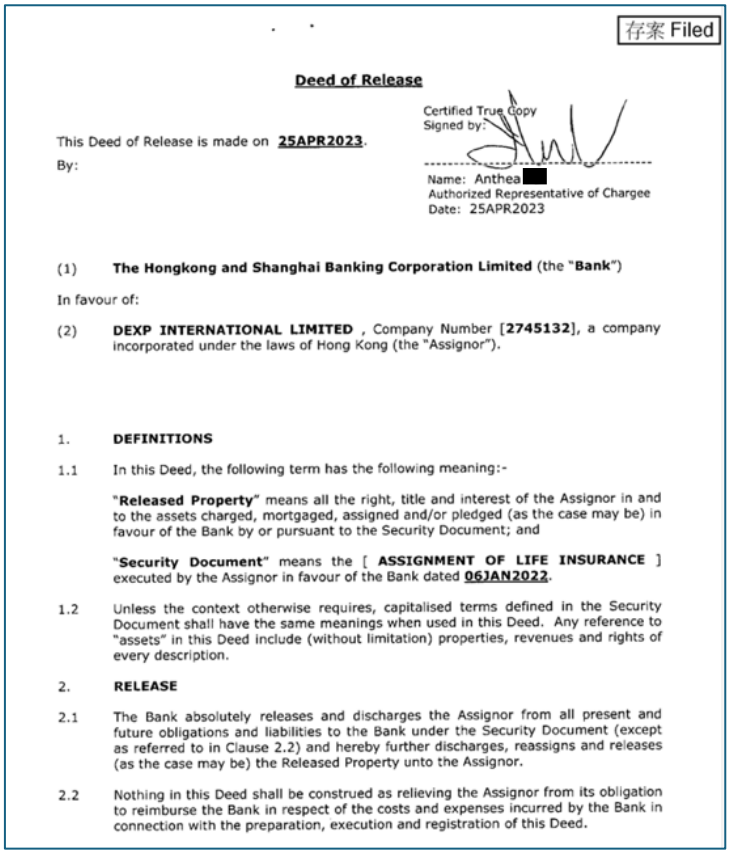
Showing the importance placed on GPUs, in August 2022 the Biden administration restricted the export of the most advanced GPUs to Russia and China due to their potential military and intelligence applications.[103] These restrictions did not include the consumer grade GPUs listed in the DEXP catalog, but consumer GPUs would still have significant military and intelligence applications and are barred from shipment to Russia under the ban on export of all dual-use goods in place since shortly after the February 2022 war began.

Stotechno's entry in the Russian Unified State Register of Legal Entities lists its activities as "wholesale trade in computers, peripheral devices for computers and software," and its director as Roman Sergeevich Konovalenko, who does not appear to operate any other company.[104]

According to its Hong Kong Companies Registry annual returns and other corporate records, DEXP's sole owner and director is a Russian citizen named Gleb Khitrin who lives in Hong Kong.[105] On April 18, 2023, the Epoch Times reported Khitrin's connection to DEXP as well as a company he owns in Shenzhen, China.[106]

A person named Gleb Khitrin appears on a sparse LinkedIn page as living or having previously lived in Repulse Bay, Hong Kong.[107] Khitrin is also a director for another Hong Kong company, Tsy Global Solutions Limited.[108] Tsy Global was incorporated on March 23, 2022, shortly after Russia's renewed invasion of Ukraine. It shares a registered address with DEXP in Hong Kong's YF Life Tower, as well as a company secretary (Asia Explorer Consultancy Limited).[109]

In January 2022, just before the invasion, Khitrin offered his HSBC life insurance policy as collateral for DEXP's HSBC banking facilities.[110] However, on April 25, 2023, just days after the Epoch Times report, HSBC issued a Deed of Release for the life insurance collateral.[111]



存案 Filed

Deed of Release

Certified True Copy
Signed by:
Name: Anthea [redacted]
Authorized Representative of Chargee
Date: 25APR2023

This Deed of Release is made on **25APR2023**.

By:

(1) **The Hongkong and Shanghai Banking Corporation Limited** (the "**Bank**")

In favour of:

(2) **DEXP INTERNATIONAL LIMITED** , Company Number [**2745132**], a company incorporated under the laws of Hong Kong (the "Assignor").

1. **DEFINITIONS**

1.1 In this Deed, the following term has the following meaning:-

"**Released Property**" means all the right, title and interest of the Assignor in and to the assets charged, mortgaged, assigned and/or pledged (as the case may be) in favour of the Bank by or pursuant to the Security Document; and

"**Security Document**" means the [**ASSIGNMENT OF LIFE INSURANCE**] executed by the Assignor in favour of the Bank dated **06JAN2022**.

1.2 Unless the context otherwise requires, capitalised terms defined in the Security Document shall have the same meanings when used in this Deed. Any reference to "assets" in this Deed include (without limitation) properties, revenues and rights of every description.

2. **RELEASE**

2.1 The Bank absolutely releases and discharges the Assignor from all present and future obligations and liabilities to the Bank under the Security Document (except as referred to in Clause 2.2) and hereby further discharges, reassigns and releases (as the case may be) the Released Property unto the Assignor.

2.2 Nothing in this Deed shall be construed as relieving the Assignor from its obligation to reimburse the Bank in respect of the costs and expenses incurred by the Bank in connection with the preparation, execution and registration of this Deed.

First page of HSBC's collateral Deed of Release issued to DEXP after news of its illicit trade broke.

While it is possible the timing is coincidental and we have been unable to confirm whether all HSBC services were ended or just the banking facility, it is likely that the Epoch Times article was flagged by HSBC's anti-money laundering procedures, leading to a decision to swiftly end the relationship with Khitrin. If so, it shows that HSBC Hong Kong is taking steps to comply with Western Ukraine sanctions, which is positive. However, it raises the question of whether HSBC should have done more to discover Khitrin and DEXP's sanctions evasion activities before they were reported in the media (see further discussion in Section VI-B-5, below).[112]

Case 5

Chipgoo Electronics Limited

Advertising and shipping U.S.-made semiconductors to sanctioned company

In many cases, Hong Kong consignors that appear in the Russian customs data are running a straightforward operation shipping Western technology to Russia openly, including to sanctioned companies, and doing little to hide their activities.

Chipgoo Electronics appears to be an example of this type of company. In the December 2023 CHPL dataset, it is the consignor in 348 cargoes, making it second on the list by number of cargoes. It is much further down the list, however, when measured by shipment value, with $94,000 worth of goods shipped during the month.[113] This discrepancy is due to the company's focus on cheaper chips such as those made by Analog Devices and Texas Instruments and the fact that many of its cargoes are low weight, indicating they contain small quantities. The highest value shipment is $12,600, purportedly consisting of pressure sensors manufactured by Infineon Technologies, but most shipments are low-value cargoes of just a few dollars, purportedly consisting of small shipments of chips.[114]

All Chipgoo shipments in the dataset went to a Russian company, Altrabeta (АЛЬТРАБЕТА), based in St Petersburg.[115] Altrabeta has been sanctioned by the U.S. government.[116] On its website,[117] Altrabeta states that it is a "research and production company" that develops and produces "television equipment, meteorological equipment, security and fire equipment, radio frequency identification systems," and other technology.

Chipgoo's origin and connection to Altrabeta is unclear. Chipgoo maintains a website where it advertises a wide range of technology components from Western and Chinese manufacturers, with logos featured from NXP, Microchip Inc, and Onsemi, among others.[118] The website lists the company's addresses in Hong Kong and Shenzhen but offers only a Hong Kong phone number.

There are two companies registered in Hong Kong under the name Chipgoo: Chipgoo Electronics Limited, and Chipgoo Technology Limited. [119] Chipgoo Electronics was registered on November 22, 2022. Chipgoo Technology was registered on March 2, 2022—just after the renewed Ukraine invasion began—as ANSMI Technology Limited, before changing its name to Chipgoo on November 7, 2023.[120]

Chipgoo Technology and Chipgoo Electronics officially have different owners, directors, and secretaries. Their secretaries are two corporate services companies, while their owners/directors are listed as Wuxin Lin (for Chipgoo Technology) and Shu Mu (for Chipgoo Electronics).[121] Wuxin Lin maintains a LinkedIn where he posts regular advertisements for Chipgoo,[122] but Shu Mi does not appear on any online records in English or Chinese as associated with Chipgoo.

Chipgoo logo and banner from Wuxin Lin's LinkedIn profile

Hong Kong As a Hub for Russian Vessels Conducting Illicit Trade

Hong Kong has also become essential to Russia's efforts to evade sanctions by offering a politically safe and corporate friendly location to set up subsidiaries for the ownership of shipping vessels. Records collected by C4ADS show 31 vessels owned or managed by Hong Kong subsidiaries of Russian companies. Three of the seven parent companies are subject to Western sanctions: Far Eastern Shipping Company (commonly known as FESCO), Sovcomflot, and Novatek OAO. Additionally, the records collected by C4ADS show that one non-sanctioned company owns a vessel, the *Zafar*, that was likely involved in a series of illicit transactions for Russia, including transporting stolen Ukrainian grain to Iran.

Hong Kong Vessel Owners/Managers with Russian Ultimate Owner

Hong Kong Shipowner	Registration Date	Company Role	Parent Company (Sanctioned in Red)	Vessels Owned
East Line Shipping Hong Kong	2006	Manager	East Line Shipping Co Ltd	SILVER DREAM
Abberton Ltd	2022	Registered Owner	**FESCO**	VELIKAN
Afanasyev Ltd	2023	Registered Owner	**FESCO**	KAPITAN AFANASYEV
Dalnegorsk Ltd	2023	Registered Owner	**FESCO**	FESCO DALNEGORSK
Diomid Ltd	2023	Registered Owner	**FESCO**	FESCO DIOMID
FESCO Ocean Management HK	2022	Manager	**FESCO**	F LANA (9328613), FESCO TRADER (9168233), HISTORY ELIZABETH
Gannet Shipping Ltd	2023	Registered Owner	**FESCO**	KAPITAN ABONOSIMOV
Laysan Ltd	2023	Registered Owner	**FESCO**	FESCO SOFIA
Trader Shipping Ltd-HKG	2023	Registered Owner	**FESCO**	FESCO TRADER
Vladivostok Ltd	2023	Registered Owner	**FESCO**	VLADIVOSTOK
Gloristar Co Ltd	1992	Registered Owner	Fortune Tanker JSC	GLORILAND (9904106), GLORISTAR (9449651)
Leading Goal Ltd	2007	Registered Owner	Fortune Tanker JSC	GLORISEA (9917402), GLORIWIND (9449649)
Presage Co Ltd	2022	Registered Owner	Norfes-Marine Service Co Ltd	CONFIDENT (9258569), SWIFT (9088744)
Uniluck Management Ltd	2013	Registered Owner	Norfes-Marine Service Co Ltd	ARK
Saam FSU Ltd	2002	Registered Owner	**Novatek OAO**	SAAM FSU
AM Asia M13 Ltd	2020	Registered Owner	PRSD-Aktiv LLC	MSC BILBAO
AM Asia M14 Ltd	2020	Registered Owner	PRSD-Aktiv LLC	MSC VALENCIA
AM Asia M6 Ltd	2019	Registered Owner	PRSD-Aktiv LLC	ZAFAR
Anchorstar Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	NIKOLAY ZADORNOV
Besento Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	ZALIV BAIKAL
Castellario Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	VIKTOR TITOV
Comitana Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	YURI SENKEVICH
Ivora Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	ZALIV VOSTOK
Kandita Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	ZALIV ANIVA
Vimena Shipping HK Ltd	2022	Registered Owner	**Sovcomflot**	VICTOR KONETSKY

Source: C4ADS

Subsidiaries of Sanctioned Russian Companies

FESCO is subject to U.K. sanctions due to its strategic significance to the Russian government in the transport sector.[123] The data collected by C4ADS shows that it owns nine Hong Kong subsidiaries that in turn own 12 vessels. Each of these 10 subsidiaries was founded in 2022 or 2023, after the February 2022 renewed Ukraine invasion. This indicates a likely strategic decision by FESCO to use Hong Kong as a safe haven from Western sanctions.

Sovcomflot, Russia's largest shipping company, is subject to U.S., E.U., U.K., Australia, and New Zealand sanctions. It was sanctioned by the U.S. in February 2024 as part of efforts to reduce Russia's revenue from oil sales.[124] However, while the sanctions froze assets of Sovcomflot, OFAC issued a general license allowing transactions with all but 14 Sovcomflot-owned crude oil tankers.[125] Bloomberg reported in April 2024 that Sovcomflot had begun changing the names of some of these 14 vessels "in order to distance themselves from listings on sanctions databases."[126]

The data gathered by C4ADS indicates that Sovcomflot has seven Hong Kong subsidiaries that each own one vessel. None of these seven vessels is on the list of the 14 sanctioned oil tankers. However, the data indicates that the seven companies were all registered in 2022 after the invasion began, suggesting that, like FESCO, Sovcomflot may be seeking to use Hong Kong as a safe haven for avoiding potentially tightening sanctions.

The third sanctioned Russian company, Novatek, is sanctioned by the U.S. and Canada. The data collected by C4ADS indicates that it owns one Hong Kong subsidiary with one vessel, the SAAM FSU. This subsidiary was founded in 2002, suggesting that this arrangement is unrelated to the current geopolitical situation.

Reported Illicit Grain Shipments of the Zafar

Hong Kong company HK AM Asia M6 Ltd owns the *Zafar*, a vessel that has operated in the Black Sea near Ukraine and in the Middle East, and was reported to have transported stolen Ukrainian grain to Iran and Russia.

HK AM Asia M6 Ltd is a subsidiary of Albatross Marine Asia Limited, which itself is a subsidiary of PRSD-Aktiv LLC.[127] PRSD-Aktiv LLC appears to itself be a subsidiary of the Ministry of Property Relations of Chelyabinsk Region, Russian Federation, according to data accessed through IHS Markit.

Both AM Asia M6 Ltd. and Albatross Marine Asia Limited changed their names on November 18, 2022. AM Asia M6 Ltd. was previously GLTK Asia M6 Limited and Albatross was previously GLTK Asia Maritime Limited.[128] GLTK (a.k.a. State Transport Leasing Company) is Russia's largest leasing company, which was sanctioned by the U.S., E.U., and U.K. in 2022.[129]

In April 2024, *Bellingcat* published evidence including satellite photos and vessel tracking info appearing to indicate that the *Zafar* had loaded stolen Ukrainian grain in the Black Sea and taken it to Iran.[130] In October 2023, according to *Bellingcat*, the *Zafar* had "gone dark" in the Black Sea after deactivating its Automated Identification System (**"AIS"**), a violation of international standards. Bellingcat presented satellite photos showing a ship that looked very similar to the *Zafar* two days later, October 17, at Sevastopol's Avlita Grain Terminal. On October 19, satellite images showed it being loaded with a brown-yellow substance—the color of grain. On November 11, the *Zafar* transited Turkey's Bosphorus Strait, where one of the authors of the Bellingcat article photographed it fully laden. Bellingcat reported that the ship transited the Suez Canal on November 18, eventually anchoring off the coast of Iran in early December, where it unloaded its cargo.

Zafar in Sevastopol's grain port on October 17, 2023 (Bellingcat.)

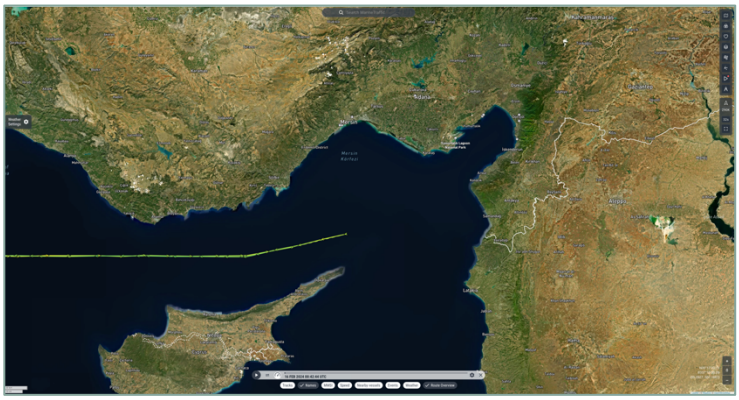
The evidence gathered by Bellingcat suggested strongly that the *Zafar* had loaded stolen Ukrainian grain and taken it to Iranian buyers, in violation of sanctions and international law.

The instance reported by *Bellingcat* was not the last time the *Zafar* transported likely stolen Ukrainian grain. In February 2023, the Ukrainian media channel *Crimean Wind* reported that satellite images showed the *Zafar* being pulled out of Sevastopol port after loading 35,800 tons of grain. On March 3, *Crimean Wind* reported that Turkey appeared for the first time to be holding up *Zafar* and other ships with stolen grain at the Bosporus Strait.[131] It is unclear, however, whether this delay was due to the stolen grain or other reasons, as it appears that Turkey did eventually allow *Zafar* to pass and reach the Middle East.

Satellite data from MarineTraffic shows that on February 19, 2024, *Zafar* was treading water near the Strait of Kerch, off the east coast of Crimea, when its position suddenly went dark around 5:02 a.m. UTC. It didn't reappear until Feb. 26 at 10:56 a.m., a full week later and several nautical miles west of its Feb. 19 position. It could easily have made the trip to Sevastopol and back in this time.

Zafar anchored near Crimea with Sevastopol in view, its last position before going dark for seven days (MarineTraffic satellite imagery)

Zafar remained in position until Feb. 28 at about 9:45 a.m., when it went dark again. It reappeared on March 1 at 1:17 a.m. on the other side of the Black Sea, awaiting entry into the Bosphorus Strait. The alleged delay reported by *Crimean Wind* only lasted four days. *Zafar* entered the Strait on March 5 and made its way to the eastern Mediterranean. On March 9 its signal disappeared again in between Cyprus and Syria. It reappeared on March 22 when it began its return to the Black Sea.


Zafar at its last known position on March 9, 2024, before disappearing. On March 22, it reappeared near the same position (MarineTraffic satellite imagery).

It has been observed in the past that ships transporting illicit goods to Iran often go dark in the eastern Mediterranean just as the *Zafar* did. It is quite possible that, like the October 2023 trip, *Zafar* again visited Iran to offload its cargo.

The *Zafar* presents a particular conundrum for the Hong Kong government. Russia's theft of Ukrainian grain is a relatively straightforward violation of Geneva Conventions, which prohibit pillaging and the unlawful appropriation of property necessary for the populations' survival including food.[132] It is easy for the government to dismiss Western sanctions as inapplicable in Hong Kong by law. It is more difficult, however, when the allegation is that a ship owned by a Hong Kong company carries stolen goods from Ukraine in violation of international law. It raises the potential for litigation that could be brought in Hong Kong to test the government's commitment to its international obligations, for example by the Ukrainian government or the owners of the grain crops.

Iran

Iranian Effort to Evade Sanctions — Overview

Iran has developed complex strategies to circumvent international sanctions imposed on its regime. These efforts involve an extensive network of front companies, financial intermediaries, and covert operations that span multiple jurisdictions, allowing sanctioned Iranian entities to continue their economic activities and generate significant revenue.

One of the primary methods used by Iran to evade sanctions is the establishment of shadow banking networks, which have been a focus of U.S. sanctions and enforcement efforts in recent years. [133] These networks consist of foreign exchange houses and front companies that operate in countries like Hong Kong, Singapore, and the UAE. Interlinked front companies enable sanctioned Iranian firms to access the international financial system and obscure their trade with foreign customers, allowing Iran to sell petrochemical products worth billions of dollars annually despite international restrictions.

Iran's sanctions evasion strategy also involves systematic, government-supported efforts to assist sanctioned entities in manipulating documents and leveraging foreign intermediaries. Iranian authorities coordinate closely with designated entities to manipulate purchase documents, customs regulations, and banking transactions. This includes practices such as not providing certificates of origin or accepting mismatched certificates from non-Iranian businesses, which help conceal the true origin of goods.[134]

Iran's efforts to bypass sanctions are not limited to financial and trade manipulations. The regime also employs a "dark fleet" of tankers to transport oil covertly. These vessels operate outside of international maritime regulations, frequently changing their names and flags to evade detection. The dark fleet is essential for Iran's continued oil exports, particularly to countries like China, which rebrand the oil to conceal its Iranian origin. These ghost ships, often old and lacking proper insurance, have been involved in numerous incidents globally, causing damage and evading responsibility due to their opaque ownership and registration practices.[135]

These elaborate and coordinated efforts by Iran underscore the regime's determination to mitigate the impact of international sanctions and sustain its economic and military activities despite global restrictions. The activities sustained by this sanctions evasion increasingly include the export of drones and other weapon systems to authoritarian governments including those in Russia and Sudan, as well as to militias across the Middle East, contributing to global instability well outside Iran's immediate region.[136]

Hong Kong's Role in Iran Sanctions Evasion

Iran employs a sophisticated network of front companies, shell corporations, and transshipment firms to disguise the origin of goods and financial transactions, with Hong Kong a leading hub for these activities. These entities assist with masking both exports and imports from and to Iran. Common activities of these front companies include rebranding Iranian oil and petrochemical products to facilitate their sale in international markets and procuring parts such as engines for UAVs and other weapons systems for reshipment to Iran.[137]

Hong Kong also serves as a critical node in the operation of the dark fleet. These vessels frequently change their names and flags, operate without transponders, and engage in ship-to-ship transfers to mask their movements and the origin of their cargo. This fleet is essential for maintaining Iran's oil exports, with Hong Kong-based companies often providing the necessary logistics and financial support.[138]

Previously Reported Instances of Hong Kong's Links to Iranian Sanctions Evasion

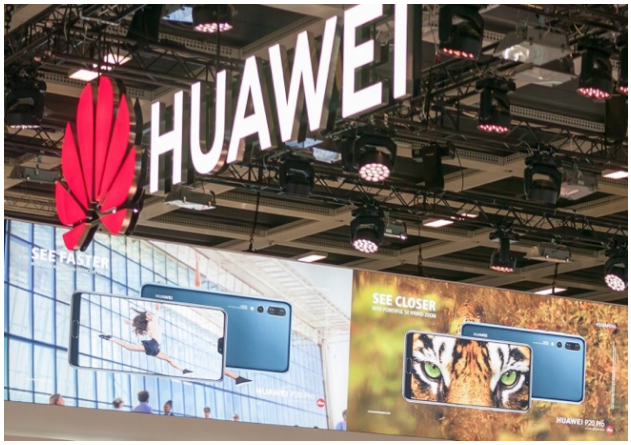
- *Hong Kong has helped Iran avoid sanctions for many years. While there have been numerous incidents reported in the media over the years, the following are the most significant and representative:*

Meng Wanzhou Affair

The Dec. 1, 2018, arrest at Vancouver International Airport of Meng Wanzhou, chief financial officer of Huawei, marked a significant escalation in the enforcement of U.S. sanctions against Iran. Charges by the U.S. Department of Justice focused on Huawei's alleged relationship with Skycom Tech Co. Ltd., a Hong Kong-based subsidiary that operated in Iran. Despite Huawei's public claims that Skycom was merely a local business partner, the U.S. government asserted—and Meng ultimately admitted as part of a Deferred Prosecution Agreement ("DPA") with the U.S.—that Skycom was effectively controlled by Huawei.[139] Meng, who served on Skycom's board from 2008 to 2009, was accused of misleading the British bank HSBC about the true nature of Huawei's relationship with Skycom, enabling Huawei to continue its business dealings with Iran in violation of U.S. sanctions.[140]

According to the DPA, HSBC's Hong Kong branch was key to the scheme because it facilitated numerous financial transactions for Huawei. Meng's false representations in 2013 to HSBC executives in Hong Kong downplayed Huawei's control over Skycom, leading the bank to process millions of dollars in transactions that would otherwise have been flagged for sanctions violations. [141] These transactions included payments from Skycom's bank accounts in Asia to entities in other countries, all of which were cleared through the U.S. financial system.[142]

The case received significant global attention, highlighting the role of Hong Kong and its financial institutions in facilitating sanctions evasion. By leveraging the city's advanced financial infrastructure and relatively lax regulatory oversight, Huawei was able to obscure its allegedly illicit activities in Iran from HSBC.



A Huawei exhibition with advertisements.

HSBC and Standard Chartered Accounts Facilitating Iran Trade

In 2022, the *Wall Street Journal* reported that "a slew of institutions" in Hong Kong and elsewhere, including the Hong Kong branches of HSBC and Standard Chartered, maintained accounts for Hong Kong companies that handled trade for sanctioned Iranian entities.[143]

The Journal's investigation uncovered documents showing a transaction in which an HSBC Hong Kong client, Scofield HK Ltd., sold restricted petrochemical products to an Indian buyer, who paid for the transaction by depositing $170,000 into Scofield's HSBC account. As for Standard Chartered, the report revealed that the bank held accounts for two Hong Kong front companies, Bobch Co., Limited, and Plus Power Co., Limited. Those companies handled illicit trade for the National Iranian Tanker Company, a subsidiary of the National Iranian Oil Company

The Scofield transactions involved the use of dual invoices—one real and one fake. The invoices were identical except that the name of the seller was changed. In the version sent to HSBC and otherwise used for official records, the seller was listed as Scofield. The second, secret version, however, listed the seller as Persian Gulf Petrochemical Industry Commercial Company.[144]

Triliance Petrochemical Network

Triliance Petrochemical Co. Ltd., a Hong Kong company, was sanctioned by the U.S. Treasury Department in January 2020 for its role in facilitating the sale of Iranian oil from the National Iranian Oil Company ("**NIOC**"). The sanctions targeted Triliance for allegedly using an extensive network of Hong Kong and global front companies to disguise its involvement in these transactions. The Treasury Department determined that this network allowed Triliance to process payments and manage shipments in a way that concealed the true Iranian origin of the oil.[145]

Since sanctioning Triliance, the U.S. government has issued 10 separate rounds of sanctions against the Triliance network of front companies, showing the extensive reach of this Hong Kong-centered operation. [146] The sanctions targeted companies globally, including 31 Hong Kong companies. The most recent round of Triliance-related sanctions was issued in March 2023, more than three years after Triliance itself was sanctioned.[147]

The extensive nature of this network and the long delay in sanctioning its affiliates reveals a key vulnerability in the sanctions regime and shows why Hong Kong makes a compelling base of operations for sanctions evasion. It currently takes U.S. government authorities at OFAC and the State Department months, if not years, to investigate and sanction a company. Yet in Hong Kong, new companies can be set up in a matter of days. There is little to stop NIOC and other sanctions targets from establishing extensive networks of front companies at will, continually creating new avenues for transferring goods and payments.

Sanctions on drone suppliers

After Russia's renewed Ukraine invasion in February 2022, the U.S. and E.U. placed increased focus on the networks used to supply Iran's UAV programs. The drones produced as part of this program have been used extensively in Ukraine and by Iranian proxies in the Middle East such as the Houthis in Yemen.

On September 27, 2023, OFAC sanctioned a group of entities for their work in procuring drone parts for Iran. Hongkong Himark Electron Model Ltd. was one of the key entities sanctioned. The company was involved in procuring servomotors and other electronic components used for the operation and control of drones. [148] Himark falsified invoices to obscure the Iranian end user and supplied significant quantities of these components to Iran and its proxies, including the Houthi rebels in Yemen.[149]

Also on September 27, 2023, BIS added Speed Business Trading (HK) Ltd. and Sunrising Logistics (HK) Ltd. to the Entity List, after finding that "these companies have procured and/or attempted to procure U.S.-origin items that would ultimately support Iran's weapons of mass destruction and UAV programs."[150]

According to the Hong Kong Corporate Registry, Speed Business Trading (Hongkong) Limited was dissolved in December 2021—almost two years before it was added to the U.S. Entity List. It is unclear why BIS added it to the entity list after its dissolution. Prior to dissolution, its director and owner was Wei Wei Li (李偉偉), a Chinese passport holder. Li holds no other directorships in Hong Kong.[151]

On February 2, 2024, the U.S. Treasury's OFAC sanctioned another network of UAV suppliers. Unlike the September sanctions, this round focused specifically on the role of Hong Kong companies in this supplier network. Three Hong Kong-based companies—FY International Trading Co., Limited, Duling Technology HK Limited, and Advantage Trading Co., Limited—were sanctioned. These entities were implicated in facilitating the procurement of dual use technology and materials for Iran's ballistic missile and UAV programs, including parts from the U.S. and E.U., with millions in payments being processed in U.S. dollars.[152]

Sanctions on Hong Kong ship owners

In February [153] and March [154] 2024, the U.S. Treasury Department sanctioned Hongkong Unitop Group Ltd, which the Treasury asserted was the owner of the ghost ship Eternal Fortune, and Cap Tees Shipping Co Limited, which it said owns the tanker Artura. These companies were alleged to be involved in ship-to-ship transfers to obscure the origin of Iranian oil. Operating under false flags and names, these vessels were alleged to be part of the network of hidden ships that are key to maintaining Iran's oil exports.[155]

U.S. Sanctions Evasion Prosecutions Involving Hong Kong's Trade with Iran

- *There have been numerous U.S. criminal actions brought against Iran sanctions evaders over the years, with many involving Hong Kong front companies and transhippers. Following is a summary of recent such actions.*

U.S. v. Hossein Hatefi Ardakani & Gary Lam

In *U.S. v. Hossein Hatefi Ardakani & Gary Lam,*[156] filed in December 2023, the defendants were charged with crimes related to the procurement of U.S.-manufactured dual-use microelectronics for Iran. Ardakani, an Iranian national, and Lam, a resident of Hong Kong and China, allegedly conspired to illegally purchase and export these components to support Iran's drone (UAV) program.

The indictment alleges that between September 2014 and September 2015, Ardakani and Lam, using a sophisticated network of front companies, procured high electron mobility transistors, monolithic microwave integrated circuit power amplifiers, and analog-to-digital converters. These components, essential for UAV production, were shipped to Hong Kong before being re-exported to Iran. This network allegedly involved multiple companies in France, Canada, and China—some aware of the ultimate buyer and some not.

U.S. v. Shaoyun Wang & Mahmood Rashid Amur Al Habsi

In *U.S. v. Shaoyun Wang & Mahmood Rashid Amur Al Habsi,*[157] the defendants were charged with facilitating the sale of Iranian oil to China via a Hong Kong company. Between December 2019 and July 2021, over $100 million worth of Iranian oil was transported to China.

The Hong Kong company through which the transactions were arranged is referred to only as Chinese Oil Company 4 (**"COC4"**). COC4 had a U.S. subsidiary, U.S. Company 7, located in Las Vegas, Nevada. According to a memorandum circulated among Revolutionary Guard officials, U.S. Company 7 acted as a "trust company" to collect funds for the Revolutionary Guard, while COC4 in Hong Kong acted as a front company to resell Iranian oil to Chinese refineries. They allegedly obtained the oil from Iran using methods including AIS (Automatic Identification System) spoofing to prevent vessel tracking and multiple ship-to-ship transfers.

Wang, who was reportedly the chair of a U.S. company in Las Vegas and the general manager of the Hong Kong-based parent company, allegedly used the Hong Kong company as a front for these transactions.[158]

U.S. v. Baoxia Liu, Yiu Wa Yung, and Yanlai Zhong

In *U.S. v. Baoxia Liu, Yiu Wa Yung, and Yanlai Zhong*,[159] the defendants were charged in a conspiracy to unlawfully export and smuggle U.S.-origin electronic components from the United States to Iran. These activities allegedly were intended to benefit entities affiliated with the Revolutionary Guard and Ministry of Defense, which oversee Iran's development and production of missiles, weapons, and military aerial equipment, including drones (UAVs).

According to the indictment, from as early as May 2007 until at least July 2020, the defendants used an array of front companies in Hong Kong and China to channel dual-use U.S.-origin items, such as electronics and components, to sanctioned Iranian entities. These components allegedly were used in the production of UAVs, ballistic missile systems, and other military applications. The indictment further alleges that the defendants' network utilized both Chinese and Hong Kong-based companies to obscure the final destination of these goods, thereby bypassing U.S. export controls and sanctions.

U.S. v. Mehdi Khoshghadam

In *U.S. v. Mehdi Khoshghadam,*[160] the defendant, who was the managing director of Pardazan System Namad Arman (PASNA), was charged with leading a sanctions evasion network that used front companies in Hong Kong to procure electronic components for Iran's defense industry, specifically for drone (UAV) production.The U.S. Department of the Treasury also sanctioned Khoshghadam and six associated entities for their roles in supporting Iran's procurement efforts.[161] Among these entities was the Hong Kong-based Arttronix International Limited, Vohom Technology (HK) Co., Limited, and Yinke (HK) Electronics Company Limited.[162] These companies allegedly facilitated the acquisition of dual-use components, which were then funneled through Hong Kong before being shipped to Iran. The components included military items such as encoder boards and various optical components.

U.S. v. Zangakani et al.

In U.S. v. Zangakani et al.,[163] ten Iranian nationals were charged with orchestrating a nearly 20-year-long scheme to evade U.S. sanctions on Iran. This extensive operation involved allegedly disguising over $300 million in transactions, including the purchase of two $25 million oil tankers, through a network of front companies and financial entities located in the San Fernando Valley, Canada, Hong Kong, and the United Arab Emirates. The scheme allegedly sought to obscure the financial activities supporting the Iranian government.

According to the indictment, a key element of this conspiracy involved the use of Hong Kong-based front companies to facilitate illegal financial transactions. Specifically, the defendants allegedly used a Hong Kong front company, Total Excellence Ltd., to secretly purchase two oil tankers worth $25 million each for Iran from a Greek businessman.

Iranian-made drone components recovered in Ukraine (U.S. Defense Intelligence Agency).

New Findings and Analysis from Open-Source Databases

Hong Kong Companies Involved in Transshipments Of UAV Parts To Iran

Iranian military kamikaze drone.

State Department statistics indicate that the majority of military UAVs used in the world today originated in Iran.[164] According to RUSI, three types of Iranian drones have been found in Ukraine: the Mohajer 6, the Shahed 131, and the Shahed 136.[165] The U.K. weapons investigation organization Conflict Armament Research dismantled destroyed versions of each of these UAVs. In a report laying out their findings, they determined that "each of these documented UAVs…is made almost exclusively of components produced by companies based in Asia, Europe, and the United States…More than 70 manufacturers based in 13 different countries produced these components, with 82 percent of them manufactured by companies based in the United States."[166]

As with Russia's transshipment strategy to obtain Western goods, Iran has relied heavily on Hong Kong companies to obtain Western parts for its UAVs.

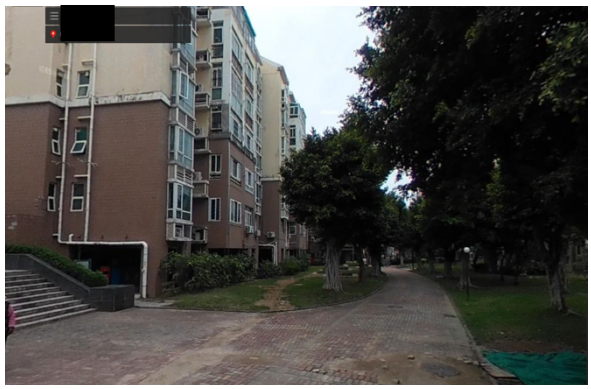
Case 1

Arttronix

Drone parts supplier dodges sanctions with new company

On April 19, 2023, OFAC sanctioned three Hong Kong companies: Arttronix International (HK) Limited, Vohom Technology (HK) Co., Ltd., and Yinke (HK) Electronics Company Limited. OFAC determined that the three companies provided various electronic goods to PASNA, an Iranian parts supplier to the military, for use in UAV programs.[167] As discussed above, these sanctions were issued simultaneously with criminal charges against an Iranian national, Mehdi Khoshghadam, for working with Arttronix, Vohom, and Yinke to import prohibited cables and connectors to Iran via Hong Kong.[168]

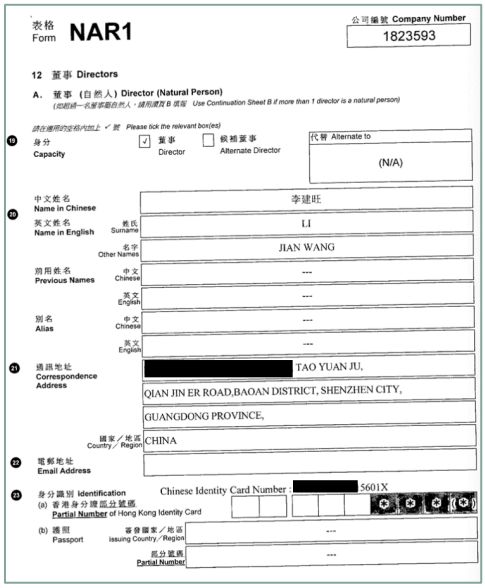
On its 2022 Annual Return (the last one it filed), Arttronix lists two owners and directors, Li Jian Wang and Liu Jing, who disclose a shared residential address in the Taoyuan Ju apartment complex in Bao An District, Shenzhen, China. Li Jian Wang's Chinese ID card number is listed in full.[169]



Li Jian Wang and Liu Jing's listed apartment building in Taoyuan Ju, Shenzhen (Baidu).

Li and Liu acted quickly after the April 19, 2023, sanctions designation. The company secretary resigned on April 21.[170] Arttronix then filed a notice with the Companies Registry declaring that on April 26, 2023, the company had convened and passed a resolution to cease operations.[171] The company made a required request to the Inland Revenue Department on April 28, 2023, seeking certification that IRD had no objection to deregistration; IRD issued the certification on January 15, 2024.[172] Shortly after on February 1, 2024, Li filed a deregistration application.[173]

Yet this was not the end for Li. A year later, on April 24, 2024, Li filed to incorporate a new company, ETS International (HK) Limited. Li is listed as the director using the same Chinese ID number.[174] However, because Chinese ID numbers are not officially entered into the Companies Registry database and Li did not provide a Hong Kong ID or passport number to register, the two companies' common director is not apparent from a Companies Registry search. It is only discoverable by pulling individual filings and comparing the ID information.



表格 Form **NAR1**

公司編號 Company Number 1823593

12 董事 Directors

A. 董事（自然人）Director (Natural Person)

Capacity: ☑ 董事 Director ☐ 候補董事 Alternate Director — 代替 Alternate to: (N/A)

中文姓名 Name in Chinese: 李建旺

英文姓名 Name in English — 姓氏 Surname: LI — 名字 Other Names: JIAN WANG

曾用姓名 Previous Names — 中文 Chinese: --- — 英文 English: ---

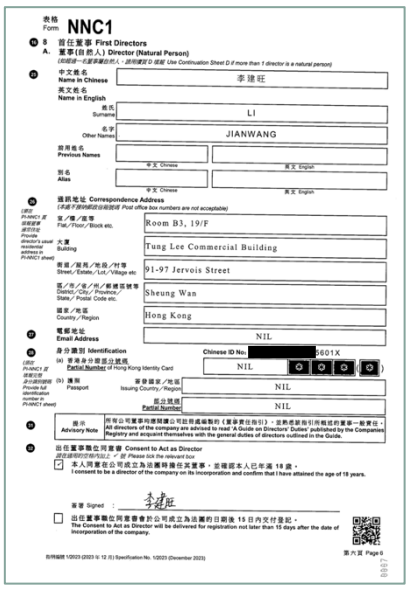
別名 Alias — 中文 Chinese: --- — 英文 English: ---

通訊地址 Correspondence Address: [redacted] TAO YUAN JU, QIAN JIN ER ROAD,BAOAN DISTRICT, SHENZHEN CITY, GUANGDONG PROVINCE, 國家／地區 Country／Region: CHINA

電郵地址 Email Address:

身分識別 Identification — (a) 香港身分證號碼 Partial Number of Hong Kong Identity Card: Chinese Identity Card Number : [redacted]5601X

(b) 護照 Passport — 簽發國家／地區 Issuing Country／Region: --- — 部分號碼 Partial Number: ---



表格 Form **NNC1**

8 首任董事 First Directors

A. 董事(自然人) Director (Natural Person)

中文姓名 Name in Chinese: 李建旺

英文姓名 Name in English — 姓氏 Surname: LI — 名字 Other Names: JIANWANG

曾用姓名 Previous Names — 中文 Chinese — 英文 English

別名 Alias — 中文 Chinese — 英文 English

通訊地址 Correspondence Address: Room B3, 19/F, Tung Lee Commercial Building, 91-97 Jervois Street, Sheung Wan, Hong Kong

電郵地址 Email Address: NIL

身分識別 Identification — Chinese ID No: [redacted]5601X

(a) 香港身分證號碼 Partial Number of Hong Kong Identity Card: NIL

(b) 護照 Passport — 簽發國家／地區 Issuing Country／Region: NIL — 部分號碼 Partial Number: NIL

提示 Advisory Note: 所有公司董事均應閱讀公司註冊處編製的《董事責任指引》，並熟悉該指引所概述的董事一般責任。All directors of the company are advised to read 'A Guide on Directors' Duties' published by the Companies Registry and acquaint themselves with the general duties of directors outlined in the Guide.

出任董事職位同意書 Consent to Act as Director

☑ 本人同意在公司成立為法團時擔任其董事，並確認本人已年滿 18 歲。 I consent to be a director of the company on its incorporation and confirm that I have attained the age of 18 years.

簽署 Signed : 李建旺

☐ 出任董事職位同意書會於公司成立為法團的日期後 15 日內交付登記。 The Consent to Act as Director will be delivered for registration not later than 15 days after the date of incorporation of the company.

Li Jianwang is listed as director in Arttronix Company records (left) and ETS company records (right); residential address and ID number redacted for this report. (Hong Kong Companies Registry).

表格 Form **NNC1**

續頁 A Continuation Sheet A

● 創辦成員詳情（第 6 項） Details of Founder Members (Section 6)

中文姓名／名稱 Name in Chinese	伍暢
英文姓名 Name in English — 姓氏 Surname	WU
名字 Other Names	CHANG
或OR 英文名稱 Name in English	NIL
地址 Address — 室／樓／座等 Flat,／Floor,／Block etc.	[redacted]
大廈 Building	
街道／屋苑／地段／村等 Street,／Estate,／Lot,／Village etc.	Taoyuanju[redacted] Qianjin 2nd Road,
區／市／省／州／鄉鎮區號等 District,／City,／ Province,／ State,／ Postal Code etc.	Bao'an District, Shenzhen, Guangdong Province
國家／地區 Country,／Region	China

認購的股本 Share Capital to be Subscribed

股份的類別 (如普通股／優先股等) Class of Shares (e.g. Ordinary,／Preference etc.)	建議向該成員發行的股份數目 Shares Proposed to be Issued to the Member		
	總數 Total Number	貨幣單位 Currency	總款額 Total Amount
ORDINARY	500	HKD	500
總值 Total	500	HKD	500

Wu Chang is listed as the sole owner of ETS, with the same address as Li Jianwang and Liu Jing (Hong Kong Companies Registry).

Liu Jing, who purportedly shared both a home and ownership of Arttronix with Li, is no longer listed as either director or owner of the new company. In fact, even Li is no longer listed as an owner. Instead, a new name appears as the sole shareholder of ETS International: Wu Chang.[175] Yet in a sign that things may not be what they seem, Wu Chang's listed home address is the same Shenzhen address that Li and Liu had listed as their residence in Arttronix's corporate filings.[176]

Apparently, none of this attracted notice from the Hong Kong Companies Registry. Showing how easy it is for even an individual whose company has been sanctioned to set up a new company in Hong Kong and continue to conduct business, the company was approved and registered just one week after applying, on May 1, 2024. It remains active, and neither ETS nor Li have been sanctioned by the U.S.[177]

Case 2

Servomotor supplier Hongkong Himark Electron Model Ltd.

Hongkong Himark Electron Model Ltd. was added to the SDN list on September 27, after OFAC determined that the company had "fulfilled several servomotor orders worth more than $1 million for PESC," an Iranian company that has procured these servomotors for UAVs. According to OFAC, Hongkong Himark sold "thousands" of these motors to both Iran and the Houthis in Yemen. In addition to Hongkong Himark, OFAC sanctioned their representative, PRC-based Fan Yang.[178]

According to the Companies Registry, Hongkong Himark was incorporated in September 2017.[179] Its two owners at founding were, and continue to be, Genhua Wang and Yifan Wang, while Genhua Wang also serves as the sole director.[180] The two owners appear to be spouses or otherwise related, as they share a residential address in Zhuhai, the Chinese city closest to Macau (and a short drive to Hong Kong).[181]

From its founding, the company secretary was SBC Corporate Services Limited in Kowloon Bay, Hong Kong.[182] In November 2023, six weeks after Hongkong Himark was added to the SDN List, SBC Corporate Services filed a notice withdrawing as corporate secretary.[183] The secretary has not been replaced, suggesting the company may be ceasing operations.[184] It has not, however, been struck from the Companies Registry and is listed as active.[185] Wang Genhua does not hold any other directorships in Hong Kong, so does not appear to have started another company to evade sanctions—at least not with himself listed as director.[186]

Notably, neither of the two owners, Genhua and Yifan Wang, were sanctioned by OFAC along with the company. The Hongkong Himark "representative" who was sanctioned, Fan Yang, does not appear in the corporate records.[187] It is possible that Fan Yang was a consultant or employee without equity in the company.

The reasons for not sanctioning the individual owners are unclear, but this situation, like the case of Li Jianwang, again underscores an ongoing challenge with U.S. sanctions in stemming the tide of illicit transshipments: it is often easier to establish evidence against corporate entities than the individuals behind the entities. But without sanctioning the individuals, the sanctions ultimately can only slow, not halt, the illicit activities of those involved.

Case 3

Chinese/Hungarian Owned Hong Kong Companies Involved in Illicit Iran Oil Deals

On Feb. 4, 2024, an anti-Iran hacker group called the PRANA Network announced that it had hacked into the email servers of Sahara Thunder, a front company for Iran's Revolutionary Guard. Shortly thereafter, this database was published on the website WikiIran.[188] The emails showed Sahara Thunder's role in facilitating petroleum sales, ship-to-ship transfers, the purchase of parts for drones and other weapons, and other illicit activities.

Two Hong Kong-based companies, HK Shipping Cooperation Limited (**"HKSC"**) and HK Petroleum Enterprises Cooperation (**"HKPEC"**), appear in the Sahara Thunder emails. As discussed below, the communications demonstrate their involvement in significant oil deals, including ship-to-ship transfers and the sale of oil originating from Oman.

Ship-to-ship transfers with HK Shipping Cooperation Limited

Based on the Sahara Thunder emails, HK Shipping Cooperation Limited appears to play an important role in brokering ship-to-ship transfers of Iranian oil. A series of Sahara Thunder emails from December 2022 detail HKSC's involvement in arranging for a vessel to receive oil from Sahara Thunder via ship-to-ship transfer.

The emails are between an unnamed representative of Sahara Thunder and "Mike" of HKSC. According to these emails, the parties are negotiating the details of a planned charter ship-to-ship transfer between a Sahara Thunder "mother vessel"—the ship that will transfer the oil—to a HKSC-arranged "daughter vessel"—the ship that will receive the oil. The negotiations appear to center around the requirements for timing and duration of the charter, the extent to which vessel documentation must be provided, and other details.

After some initial back and forth, the emails show HKSC sending a "quotation from the ship owner" with key information on the proposed agreement:

- Vessel is M/T MAREN, a tanker.
- Loading location is listed as Basrah or Khor Al Zubair Iraq, but specifically notes "Always excluding Iran."
- Discharge location: Safe ports in either Malaysia or Qingdao-Dalian range, at the charter Sahara Thunder's option.
- Loading date: 9-11 December 2022 (just two days after this email)
- Cost: 7-9mm USD for 1 port to 1 port ("BSS 1/1")

Mail December 7, 2022

title: Re: Voyage Charter for VLCC

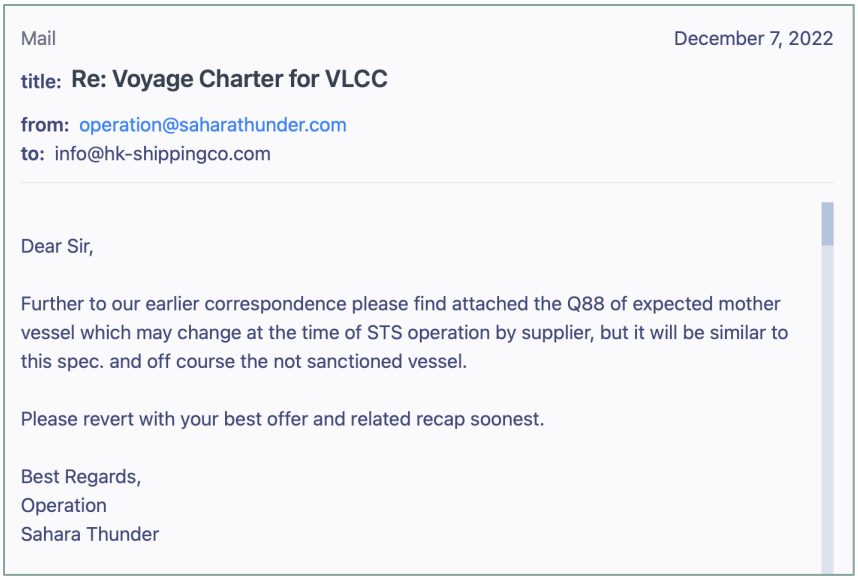
from: Info <info@hk-shippingco.com>
to: operation@saharathunder.com

VESSEL : M/T "MAREN"
CARGO : CHOPT UPTO FULL CARGO NO HEAT CRUDE OIL
GRADES : 1 GRADE WVNS
LOAD : 1 SAFE STS OPL BASRAH, IRAQ OR IN CHOPT
1 SAFE STS OPL KHOR AL ZUBAIR, IRAQ
ALWAYS EXCLUDING IRAN
DISCHARGE : 1 SP/B/STS MALAYSIA OR IN CHOPT
1 SP/B QINGDAO-DALIAN RANGE, CHINA
ALWAYS EXCLUDING CHINESE RIVER PORTS
LAYCAN : 09-11 DECEMBER 2022 (0001-2359)
FREIGHT : FOR MALAYSIA OPTION LUMPSUM USD 7,000,000 BSS 1/1
FOR CHINA OPTION LUMPSUM USD 9,000,000 BSS 1/1
30% OF THE FREIGHT TO BE PAID UPON LIFTING OF SUBJECTS
BALANCE FREIGHT TO BE PAID BBB
DEMURRAGE : USD 130,000 PDPR

◂ *HKSC email to Sahara Thunder with proposed charter details (WikiIran).*

The parties continue to negotiate terms, with Sahara Thunder pressing for a "3+3 TC" (believed to mean a three-month charter with a three-month possible extension) instead of a "voyage charter" (an agreement for a single voyage).[189] Ultimately, HKCC relays that after speaking to the vessel owner, they "accept trial voyage as voyage charter, and after that can sign 3+3 TC." [190] This exchange indicates that Sahara Thunder intends this arrangement to be ongoing and involve multiple voyages with the chartered vessel.

At several points in the email exchange, the parties refer to the HKSC vessel having a "clean flag." This appears to be important to Sahara Thunder. "Clean flag" refers to a requirement that the vessel not be under sanctions or restrictions. In a December 7, 2022, email, the Sahara Thunder representative provides a Q88 (vessel documentation) of the expected mother vessel and explicitly states that it is "the not sanctioned vessel."



Mail December 7, 2022

title: **Re: Voyage Charter for VLCC**

from: operation@saharathunder.com
to: info@hk-shippingco.com

Dear Sir,

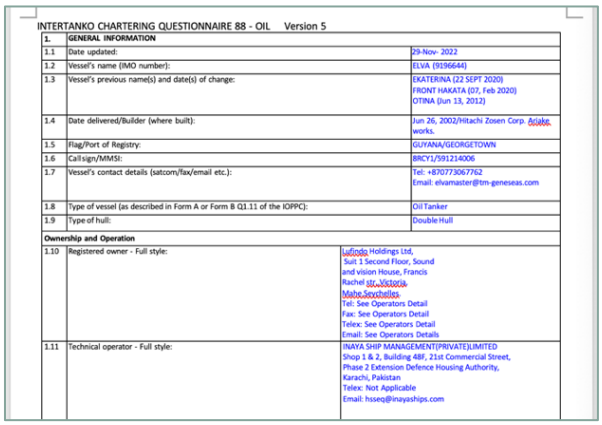
Further to our earlier correspondence please find attached the Q88 of expected mother vessel which may change at the time of STS operation by supplier, but it will be similar to this spec. and off course the not sanctioned vessel.

Please revert with your best offer and related recap soonest.

Best Regards,
Operation
Sahara Thunder

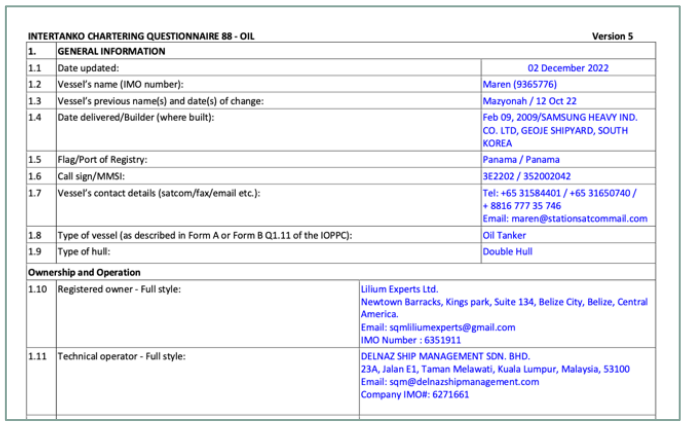
◂ *Sahara Thunder specifies that it will be providing "the not sanctioned vessel" for the ship-to-ship transfer (WikiIran).*

Attached to the same email is the Q88 (a standardized vessel chartering questionnaire) for the vessel Sahara Thunder expects to serve as the mother vessel, though the emailer notes that this could change. The vessel is the *Elva*, which the Q88 indicates is a Guyana-flagged oil tanker with a Seychelles company listed as the owner. In another email, HKSC provides the Q88 for the *Maren*. Maren is listed in the Q88 as Panama-flagged with a Belize corporate owner.



INTERTANKO CHARTERING QUESTIONNAIRE 88 - OIL Version 5

1.	**GENERAL INFORMATION**	
1.1	Date updated:	29-Nov- 2022
1.2	Vessel's name (IMO number):	ELVA (9196644)
1.3	Vessel's previous name(s) and date(s) of change:	EKATERINA (22 SEPT 2020) FRONT HAKATA (07, Feb 2020) OTINA (Jun 13, 2012)
1.4	Date delivered/Builder (where built):	Jun 26, 2002/Hitachi Zosen Corp. Ariake works.
1.5	Flag/Port of Registry:	GUYANA/GEORGETOWN
1.6	Call sign/MMSI:	8RCY1/591214006
1.7	Vessel's contact details (satcom/fax/email etc.):	Tel: +870773067762 Email: elvamaster@tm-geneseas.com
1.8	Type of vessel (as described in Form A or Form B Q1.11 of the IOPPC):	Oil Tanker
1.9	Type of hull:	Double Hull
Ownership and Operation		
1.10	Registered owner - Full style:	Lufindo Holdings Ltd, Suit 1 Second Floor, Sound and vision House, Francis Rachel str, Victoria, Mahe,Seychelles Tel: See Operators Detail Fax: See Operators Detail Telex: See Operators Detail Email: See Operators Details
1.11	Technical operator - Full style:	INAYA SHIP MANAGEMENT(PRIVATE)LIMITED Shop 1 & 2, Building 48F, 21st Commercial Street, Phase 2 Extension Defence Housing Authority, Karachi, Pakistan Telex: Not Applicable Email: hsseq@inayaships.com



INTERTANKO CHARTERING QUESTIONNAIRE 88 - OIL Version 5

1.	**GENERAL INFORMATION**	
1.1	Date updated:	02 December 2022
1.2	Vessel's name (IMO number):	Maren (9365776)
1.3	Vessel's previous name(s) and date(s) of change:	Mazyonah / 12 Oct 22
1.4	Date delivered/Builder (where built):	Feb 09, 2009/SAMSUNG HEAVY IND. CO. LTD, GEOJE SHIPYARD, SOUTH KOREA
1.5	Flag/Port of Registry:	Panama / Panama
1.6	Call sign/MMSI:	3E2202 / 352002042
1.7	Vessel's contact details (satcom/fax/email etc.):	Tel: +65 31584401 / +65 31650740 / + 8816 777 35 746 Email: maren@stationsatcommail.com
1.8	Type of vessel (as described in Form A or Form B Q1.11 of the IOPPC):	Oil Tanker
1.9	Type of hull:	Double Hull
Ownership and Operation		
1.10	Registered owner - Full style:	Lilium Experts Ltd. Newtown Barracks, Kings park, Suite 134, Belize City, Belize, Central America. Email: sqmliliumexperts@gmail.com IMO Number : 6351911
1.11	Technical operator - Full style:	DELNAZ SHIP MANAGEMENT SDN. BHD. 23A, Jalan E1, Taman Melawati, Kuala Lumpur, Malaysia, 53100 Email: sqm@delnazshipmanagement.com Company IMO#: 6271661

Proposed vessel details for Elva and Maren provided by Sahara Thunder and HKSC (WikiIran).

Throughout the negotiations, Sahara Thunder's representative expressed concerns about the length and nature of the charter, never fully agreeing to the "trial voyage" followed by a 3+3 TC proposed by HKCC.

Ultimately, the deal may not have been finalized. There is nothing in the email leak showing final terms. Additionally, according to records and maps of the *Maren*'s movements collected by C4ADS, it remained in the Middle East for the next several months, not reaching Asia until February 2023. However, Iran has been known to mask its trail of oil shipments by conducting multiple ship-to-ship transfers and other maneuvers within a single voyage. It is therefore impossible to rule out *Maren's* involvement.

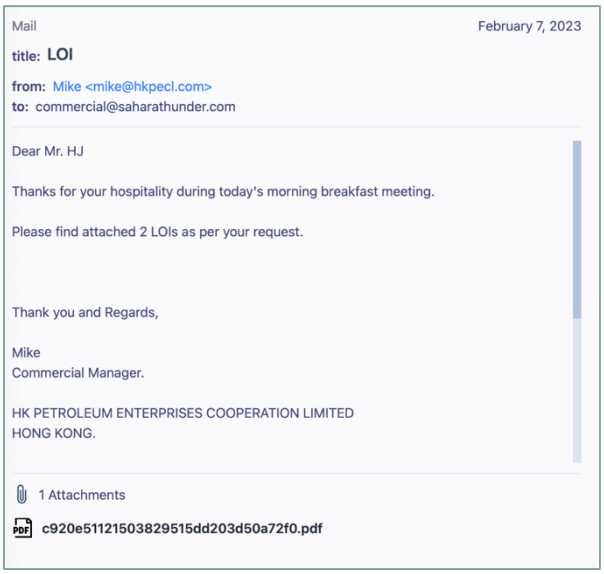
Crude oil sales with HK Petroleum Enterprises Cooperation Limited

Another email in the Sahara Thunder data leak, subject line "LOI," for "Letter of Intent," was sent by "Mike" at HK Petroleum Enterprises Cooperation Limited, with an email address of mike@hkpecl.com. Mike emails "Mr. HJ" at the address commercial@saharathunder.com and indicates that the two had met that morning for breakfast. Mike then indicates that there are two letters of intent attached.

The attached LOIs detail significant purchase agreements for heavy crude oil from Oman. The letterhead includes an address for PECL in Kwun Tong, Kowloon, and a telephone number with Hong Kong's +852 country code. The documents are signed by 陳敏—Chen Min. The LOIs are addressed to "TSCO," which could be affiliated with Sahara Thunder since these LOIs were sent to a Sahara Thunder address.

The two LOIs specify the purchase of 4,000,000 and 1,000,000 barrels per month of crude oil. The delivery for both LOIs is scheduled to begin in mid-February 2023, with the first LOI continuing for 12 months. Like the arrangements in the separate HKSC email chain, the terms of delivery for both LOIs include ship-to-ship transfers in the Persian Gulf, with the oil discharged in Malaysia or China. Both LOIs require that the transfer only occur "with clean mother vessel and clean documents"—indicating a focus on non-sanctioned vessels.

The domain hkpecl.com, from which Mike sent his email, currently contains only an empty index folder. In an archived version from December 2021, the website contained only the logo for HKPEC (the same one that appears on the LOIs). The website does not appear to have ever been developed further.



Mail February 7, 2023

title: LOI

from: Mike <mike@hkpecl.com>
to: commercial@saharathunder.com

Dear Mr. HJ

Thanks for your hospitality during today's morning breakfast meeting.

Please find attached 2 LOIs as per your request.

Thank you and Regards,

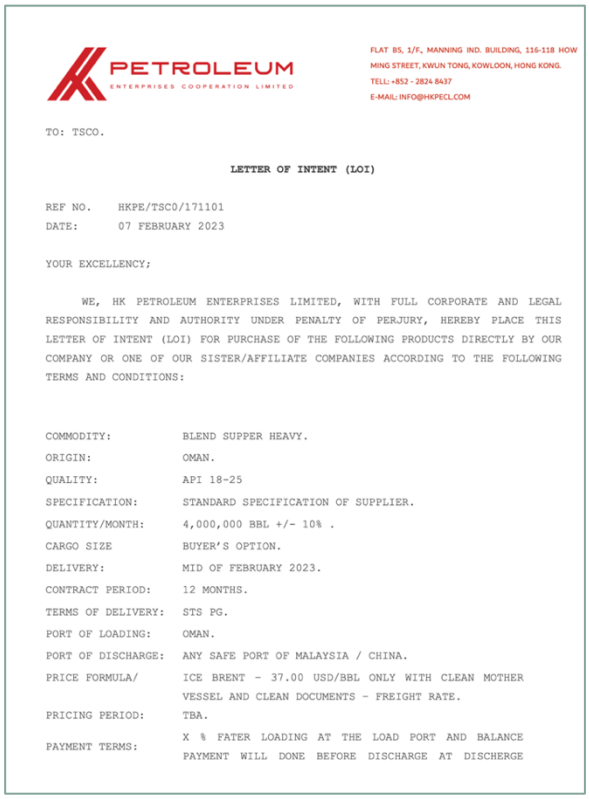
Mike
Commercial Manager.

HK PETROLEUM ENTERPRISES COOPERATION LIMITED
HONG KONG.

1 Attachments

c920e51121503829515dd203d50a72f0.pdf

Email from "Mike" at HKPEC to Sahara Thunder's HJ indicating they had an in-person meeting and attaching heavy crude oil letters of intent.



PETROLEUM
ENTERPRISES COOPERATION LIMITED

FLAT B5, 1/F., MANNING IND. BUILDING, 116-118 HOW MING STREET, KWUN TONG, KOWLOON, HONG KONG.
TELL: +852 - 2824 8437
E-MAIL: INFO@HKPECL.COM

TO: TSCO.

LETTER OF INTENT (LOI)

REF NO. HKPE/TSCO/171101
DATE: 07 FEBRUARY 2023

YOUR EXCELLENCY;

WE, HK PETROLEUM ENTERPRISES LIMITED, WITH FULL CORPORATE AND LEGAL RESPONSIBILITY AND AUTHORITY UNDER PENALTY OF PERJURY, HEREBY PLACE THIS LETTER OF INTENT (LOI) FOR PURCHASE OF THE FOLLOWING PRODUCTS DIRECTLY BY OUR COMPANY OR ONE OF OUR SISTER/AFFILIATE COMPANIES ACCORDING TO THE FOLLOWING TERMS AND CONDITIONS:

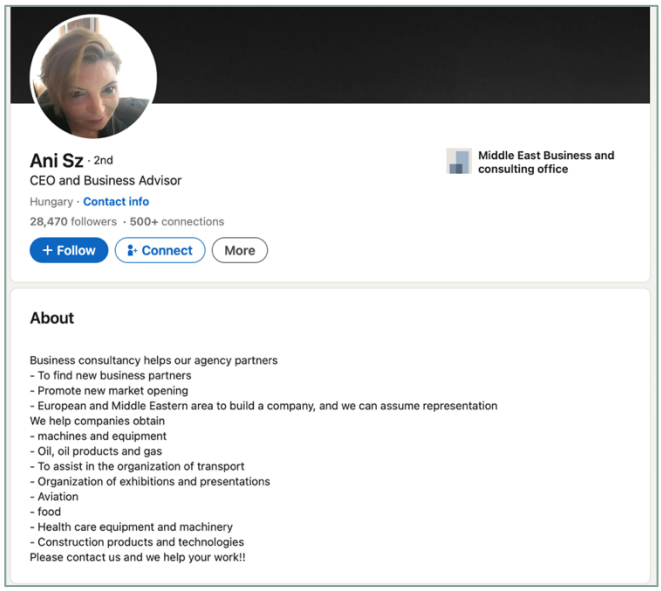
COMMODITY:	BLEND SUPPER HEAVY.
ORIGIN:	OMAN.
QUALITY:	API 18-25
SPECIFICATION:	STANDARD SPECIFICATION OF SUPPLIER.
QUANTITY/MONTH:	4,000,000 BBL +/- 10% .
CARGO SIZE	BUYER'S OPTION.
DELIVERY:	MID OF FEBRUARY 2023.
CONTRACT PERIOD:	12 MONTHS.
TERMS OF DELIVERY:	STS PG.
PORT OF LOADING:	OMAN.
PORT OF DISCHARGE:	ANY SAFE PORT OF MALAYSIA / CHINA.
PRICE FORMULA/	ICE BRENT - 37.00 USD/BBL ONLY WITH CLEAN MOTHER VESSEL AND CLEAN DOCUMENTS - FREIGHT RATE.
PRICING PERIOD:	TBA.
PAYMENT TERMS:	X % FATER LOADING AT THE LOAD PORT AND BALANCE PAYMENT WILL DONE BEFORE DISCHARGE AT DISCHERGE

First page of the letters of intent for crude oil on HKPEC letterhead.

The Chinese and Hungarian individuals associated with HKSC and HKPEC

Both HKPEC and HKSC were founded in 2021 and have the same two shareholders, same director, same company secretary, and same registered office. The company secretary and registered office is a corporate services company, Supreme Hong Kong Registration Limited. The two directors and equal shareholders are Chen Min (who signed the HKPEC LOIs) and Anett Szilagyine Szeplaki.[191]

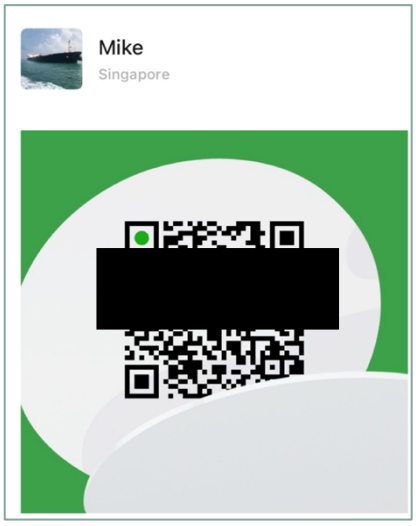
Szeplaki lists a Hungarian passport on HKPEC and HKSC corporate documents, and she maintains a LinkedIn indicating her location as Hungary.[192] This LinkedIn account appears to use an alias. It previously used her real name, as evidenced by old posts in which she was tagged under her real name, including one tag from a man based in Iran.[193] On the LinkedIn profile, Szeplaki lists her job as "General Manager, Middle East Business and consulting office," with her work location as Iran. Her "About" section includes a bulleted list of her business consultancy work, including helping companies obtain "machines and equipment," "oil, oil products and gas," and "assist in the organization of transport."



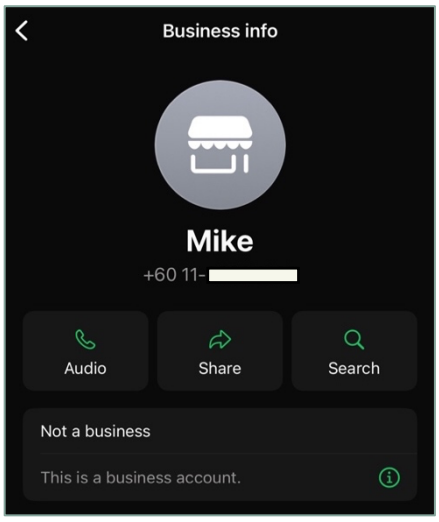
Anett Szeplaki's LinkedIn profile.

Less information is available on Chen Min, who may or may not be the "Mike" in the emails. In a Dec. 8, 2022, exchange with Sahara Thunder, "Mike" provided a QR code, which leads to his contact information on WhatsApp with a number that uses a Malaysia country code (+60). In the same email, "Mike" provides a WeChat QR code that links to an account with a picture of a tanker and lists his location as Singapore. The corporate documents for these companies, however, list a China passport for Chen Min.[194]

On Feb. 2, 2024 – just two days before hackers exposed the Sahara Thunder emails – Chen Min set up a new company called HK Energy Corporation Limited. According to the incorporation form, the company is owned by HKSC, with Chen as its only director. Szeplaki is not mentioned.[195]



"Mike's" WeChat (left) profile.



"Mike's" WhatsApp profile.

Case 4

Orient Source (HK) Ltd.

Request to Purchase Light Crude from Sahara Thunder

The Sahara Thunder hacked emails show that on Jan. 5, 2023, Navin Tauro, the Director of Singaporean company Orion Silver Pte. Ltd., emailed Sahara Thunder "on behalf of Orient Source (HK) Ltd." to provide a "letter from Orient Source requesting for a sale-purchase offer on light crude oil." The email indicates that this letter is the result of Sahara Thunder's meeting on Dec. 17, 2022, with "Dr Moosavi, Mr. Allahverdiha and Mr. Babakhani, representing our interest."

The email attaches a letter on Orient Source letterhead, dated Jan. 5, 2023, and addressed to "M/S Sahara Thunder" in Tehran, Iran. The four names noted in the email above are listed in the "Via" line. The letter is signed by "Mr. Alistair Sean Jeffries, CEO/Founder – Orient Source (HK) Limited."

ORIENT SOURCE (HK) LIMITED
QUALITY SOURCING SOLUTIONS

ADDRESS: SUITES 01-08 , 27F , SHUI ON CENTRE , 6-8 HARBOUR ROAD WANCHAI, HONG KONG
WWW.ORIENT-SOURCE.COM

DATE : JAN 05TH, 2023
REF NO : OSHK/NIOC/LTR-230105-11001-PROJECT 7

TO:
M/S SAHARA THUNDER,
ADDRESS : NO.2- MOGHADAS ALLEY (6)- GHASIR ST-
BEHESHTI ST, TEHRAN
IRAN

VIA : MR NAVIN TAURO / DR MOOSAVI / MR. ALLAHVERDIHA / MR. BABAKHANI

SUB : REQUEST FOR A SALE & PURCHASE OFFER FOR LIGHT CRUDES (API 33-35 AND API 29-31)
AT STS / TTO MALAYSIA T&CS

DEAR SIR(S),

REFER YOUR MEETING ON 17TH DECEMBER 2022 WITH DR MOOSAVI, MR. ALLAHVERDIHA AND MR. BABAKHANI AND THE DISCUSSION HAD ON THE ABOVE SUBJECT.

WE ARE KEEN TO RECEIVE A FIRM OFFER FROM YOU , FOR SALE AND PURCHASE OF LIGHT CRUDE OILS (API 33-35 & API 29-31) IF AVAILABLE AND AT MALAYSIA AND AS PER THE BELOW ;

1. PRODUCT – API 33-35 AND API 29-31
2. QUANTITY - 500,000 BBLS TO 2 MILLION BARRELS FOR A SPOT TRIAL FIRST ORDER
3. QUANTITY – 2MILLION TO 4MILLION BARRELS A MONTH X 12 -24 MONTHS
4. STS/CIF IN MALAYSIA WATERS, INDIA WEST COAST, MEDITERREAN OR CHINA WATERS

PAYMENT TERMS :

1. IF PRESENTED WITH A VALID AND FRESH QNQ WITH VESSEL LOAD PORT CARGO & SHIPPING DOCUMENTS WE CAN PAY 100% WITHIN 72HRS AND THEN MOVE TO STS/LIFT THE PRODUCT.
2. IF BUYER IS ALLOWED TO CONDUCT A QNQ ONBOARD THE SELLER VESSEL WE WILL PAY 100% WITHIN 72HRS OF THE QNQ REPORT AND THEN MOVE TO STS/LIFT THE PRODUCT.
3. A BANK GUARANTEE FOR ONE SHIPMENT AMOUNT CAN BE PROVIDED ON THE ANNUAL FIXED CONTRACT EXECUTED BETWEEN THE PARTIES.
4. PAYMENTS CAN BE MADE IN AED, EUROS, CRYPTO OR CHINESE YUAN.

WE CONFIRM THAT WE HAVE THE NECESSARY EXPERIENCE, PERSONNEL, FINANCES AND LOGISTICS TO UNDERGO SUCH COMMERCIAL PURCHASE OPERATIONS AND FOR THE ABOVE MENTIONED PRODUCT AND ON AN IMMEDIATE BASIS.

THANK YOU !!

OSHK/V22.190

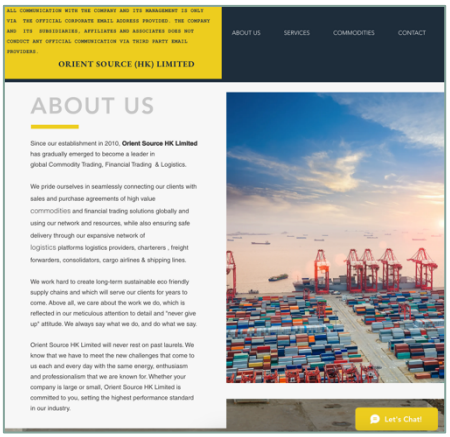
MR. ALISTAIR SEAN JEFFRIES
CEO / FOUNDER – ORIENT SOURCE (HK) LIMITED

OSHK/V22.190 STRICTLY CONFIDENTIAL 1

Letter from Alistair Jeffries of Orient Source to Sahara Thunder.

Corporate records indicate Orient Source (HK) Limited was formed in August 2014.[196] The company maintains a website, however, where it states it was established in 2010 and is "a leader in global Commodity Trading, Financial Trading & Logistics."[197] The website describes its activities as "connecting our clients with sales and purchase agreements of high value commodities and financial trading solutions globally." The site lists the company's head office in Wanchai, Hong Kong.

The purported CEO, Alistair Jeffries, is listed as the sole owner and director of the company.[198] He has an account on X (formerly Twitter), which has not been updated since 2013.[199] The latest annual return for the company (2023) describes Jeffries as a citizen of India.[200] The original incorporation form filed in 2014 lists an address in Mumbai. His X account, however, listed his location as China.



ORIENT SOURCE (HK) LIMITED
ABOUT US SERVICES COMMODITIES CONTACT

ABOUT US

Since our establishment in 2010, **Orient Source HK Limited** has gradually emerged to become a leader in global Commodity Trading, Financial Trading & Logistics.

We pride ourselves in seamlessly connecting our clients with sales and purchase agreements of high value commodities and financial trading solutions globally and using our network and resources, while also ensuring safe delivery through our expansive network of logistics platforms logistics providers, charterers , freight forwarders, consolidators, cargo airlines & shipping lines.

We work hard to create long-term sustainable eco friendly supply chains and which will serve our clients for years to come. Above all, we care about the work we do, which is reflected in our meticulous attention to detail and "never give up" attitude. We always say what we do, and do what we say.

Orient Source HK Limited will never rest on past laurels. We know that we have to meet the new challenges that come to us each and every day with the same energy, enthusiasm and professionalism that we are known for. Whether your company is large or small, Orient Source HK Limited is committed to you, setting the highest performance standard in our industry.

Let's Chat!

Orient Source website's "About Us."

Profile photo on X (Twitter) account attributed to Alistair Jeffries.

North Korea

North Korean Efforts to Evade Sanctions — Overview

Like Iran and Russia, North Korea has developed various strategies to evade international sanctions, allowing it to sustain its economy and continue its nuclear and ballistic missile programs despite extensive global restrictions.

North Korea engages regularly in illicit ship-to-ship transfers to import refined petroleum and export coal, circumventing U.N. sanctions. These transfers often occur in international waters, involving a network of shipbrokers, trading companies, and maritime operators that obscure the transactions' true nature. North Korean vessels frequently change names and flags to evade detection.[201]

North Korea employs complex ownership structures and trusted third-party intermediaries to maintain access to the global financial system. These intermediaries operate through front companies and shell entities, often using aliases and frequently changing locations to avoid detection by international regulators. This network supports North Korea's ability to acquire dual-use and restricted technologies necessary for its military and nuclear capabilities, as well as its sales of resources to generate much-needed hard currency for the regime.[202]

North Korea has also made extensive use of hacking for cybertheft and blackmail. North Korean hacking groups linked to the regime have been involved in high-profile cyber heists, including a theft of $81 million from Bangladesh's central bank and significant sums from cryptocurrency exchanges and banks worldwide.[203] These cyber activities have netted North Korea billions of dollars, which are funneled back to support its weapons programs and regime stability.[204]

Hong Kong's Role in North Korea Sanctions Evasion

Hong Kong is critical to North Korea's sanctions evasion efforts. As with Russia and Iran, North Korea operates or associates with a network of Hong Kong shell companies designed to mask illicit operations. These shell companies operate oil tankers and other vessels that provide resources and other goods to North Korea, in turn receiving coal and North Korean resources for export. Hong Kong has also been used to launder North Korea's stolen crypto assets.

U.N. Sanctions Enforcement in Hong Kong

Hong Kong is required under its own laws and treaties to abide by the U.N. sanctions on North Korea (though not the more extensive sanctions imposed by the U.S., E.U., and their allies). There is little evidence, however, that the city has sought to consistently enforce these obligations.

Hong Kong implements the U.N.'s North Korea sanctions via a local regulation, the United Nations Sanctions (Democratic People's Republic of Korea) Regulation, [205] and the Commerce and Economic Development Bureau maintains lists of both sanctioned persons and sanctioned vessels.[206]

Under the DPRK Regulation, anyone who contravenes the sanctions is subject to up to seven years in prison and an unlimited fine. Any person who contravenes entry bans for sanctioned persons is subject to a fine and imprisonment up to two years.

Both of the Commerce and Economic Development Bureau's sanctions lists are identical to corresponding lists published by the U.N. Like the U.N. lists, they mostly include North Korean individuals and companies, rather than foreign sanctions evaders or facilitators.[207] Notably, however, of the 12 non-DPRK entities on the U.N.'s sanctioned persons list, four are

from Hong Kong—more than any other country—with three additional from mainland China.

Further showing the important role of Chinese and Hong Kong companies in illicit North Korea trade, on the U.S. SDN List there are 479 persons listed under the various DPRK sanctions programs (though that does not account for North Koreans sanctioned under terrorist financing and other non-DPRK-specific sanctions programs). Of the 479 persons, at least 164 are from North Korea, while 94 are from China and at least 11 are from Hong Kong.[208]

Despite Hong Kong's legal commitment to enforce the U.N. DPRK sanctions, there is little evidence the government has sought to do so. With respect to the four entities sanctioned by the U.N. [209] —and thus appearing on Hong Kong's own sanctions list—corporate records do not indicate any action was taken after the designations.

Leader (Hong Kong) International Trading Limited, for example, was designated by the U.N. in 2008 for "facilitat[ing] shipments on behalf of the Korea Mining Development Trading Corporation (KOMID).[210] KOMID was designated by the UNSC in April 2009 and is the DPRK's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons." [211] Yet the company continued in operation, filing annual returns each year through 2013.[212] The company was only dissolved in August 2016 through "striking off," a process by which the Companies Registry terminates companies that have ceased operation voluntarily.[213] A search of court records also finds no civil or criminal action launched against the company.[214]

Hong Kong-Related Incidents Documented by the UNSC's North Korea Committee and Global Media

The UNSC Committee's twice-yearly reports,[215] have been instrumental in documenting and exposing North Korea's efforts to evade international sanctions, with Hong Kong making regular appearances in the Committee's detailed findings. In particular, the reports have consistently revealed the involvement of Hong Kong-registered entities in North Korea's sanctions evasion strategies, highlighting Hong Kong's role as a hub for financial transactions, procurement of dual-use technologies, and illicit shipping operations. Despite having a legal obligation to comply with the U.N. sanctions, the Hong Kong and Chinese governments have taken little apparent action against the companies or individuals involved.

Following is a sampling of some of the notable Hong Kong companies and vessels tracked by these reports.

The New Konk Saga

Multiple Hong Kong companies have been involved in the illicit activities of the *New Konk*, a vessel used to make illicit ship-to-ship oil transfers, create fraudulent ship identities, and launder proceeds using shell companies. The *New Konk* has appeared repeatedly in the UNSC Committee's reports over the years, but the vessel remains in operation.

In its March 2020 report, the Committee revealed June 2019 photographs of a vessel, the *Vifine,* conducting a ship-to-ship transfer with the *New Konk* in the East China Sea.[216] According to the Committee report, the *Vifine* was owned by a Hong Kong company, Hongxin International Ship Management Co. Limited, while the *New Konk* was owned by another Hong Kong company, New Konk Ocean International Company Limited. According to the Committee report, however, both companies shared the same Hong Kong address, indicating that they were likely alter egos for the same beneficial owner. The two ships also shared a common operator, a third Hong Kong company called All Sefety *[sic]* Ocean International Trading Co. Limited.[217]

In its August 2020 interim report, the Committee expanded on these findings. In particular, it found that in addition to its previously reported participation in ship-to-ship transfers, the *New Konk* had delivered illicit cargo directly to the North Korean city of Nampo on at least six occasions from January to May 2020.[218]

Photo of Vifine and New Konk conducting a ship-to-ship transfer (UNSC DPRK Sanctions Committee).

In March 2021, the New York Times, in a joint report with C4ADS and RUSI, revealed that despite being named in the UNSC Committee report a year earlier and recommended for a global port ban, the *New Konk* had continued its activities unabated and had entered ports in China without issue.[219] The report revealed satellite images of *New Konk* in a port Ningde,

New Konk in Ningde, China (The New York Times).

China, on January 1, 2021.

In its March 2021 report, the UNSC Committee concluded that the *New Konk*, in efforts to evade detection, had begun transmitting a fraudulent vessel identification registered to a Panama-flagged vessel, *Mouson 328*, which had been deleted from the Panama registry. The original *Mouson 328*, in turn, had been photographed in North Korea's waters in 2019. *Mouson 328* had laundered a different identity, the newly registered *Cherry 19* (which apparently never existed), then used the *Cherry 19*'s fraudulent documentation to launder yet another ship's identity, the *Smooth Sea 29*. Once *Mouson 328* had laundered these identities, it freed up the *New Konk* to transmit as the *Mouson 328* without raising red flags revealing the swap.[220]

The March 2022 UNSC Committee report revealed that *New Konk* was now owned by yet another Hong Kong company, Brilliant Trade International Co. Ltd. Brilliant Trade, formed in August 2019, [221] was registered as owning the ship *F Lonline*, but *F Lonline* was merely the newest laundered identity of *New Konk*. The vessel laundering process was complex: A Thailand-flagged vessel, *Smooth Sea 3*, was officially transferred to another company and later renamed the *F Lonline*. However, the *Smooth Sea 3* was never actually transferred. A supposedly newly built Thai vessel, *Smooth Sea 30*, was believed to be the former *Smooth Sea 3*. The title to *Smooth Sea 3*—now unconnected with any real ship—was then transferred to Rui He HK Marine Co. Ltd. It was passed on three months later to Hong Kong company Cheng Xin Shipping Ltd, reflagged under Belize and renamed *F Lonline*. The name could then be assigned to ships like the *New Konk* and swapped out as needed.[222]

Cheng Xin, the latest owner of the *New Konk*, had already been associated with another case of vessel identity laundering in the September 2021 Committee report,[223] but continued to operate freely as a Hong Kong company. In fact, even as the Committee continued to track the *New Konk* in its subsequent reports, the Hong Kong government took no action against *any* of the Hong Kong companies involved in this complex web of ship owners and managers.

The illicit activities of the *New Konk* continued unabated and appear to continue even today. The September 2023 report revealed *New Konk's* use of a new type of location tampering, known as geo-spoofing, to give the impression that it was located elsewhere. On April 4, 2023, for example, the *New Konk* (as *F Lonline*) transmitted that it was transiting the Taiwan Strait into the South China Sea. Satellite images, however, showed the vessel in Sansha Bay, China, at the time.[224]

Use of Hong Kong to Launder Stolen Cryptocurrency

North Korea's regime has long used cybertheft as a means of evading sanctions and raising money for both the regime and its illicit weapons programs. In its September 2023 report, the UNSC Committee disclosed its investigation into the use of Hong Kong front companies to launder cryptocurrency stolen by North Korea. The Committee alleged that Chinese national Wu Huihui and Hong Kong resident Cheng Hung Man used the front companies to exchange the cryptocurrency for fiat currency.[225]

In April 2023, as this investigation had been ongoing, the U.S. sanctioned Wu and Cheng along with their North Korean handler, while simultaneously charging Wu with operating as an unlicensed trader.[226] These filings revealed further details about the scheme. According to the indictments, the laundered cryptocurrency was stolen by the Lazarus Group, a hacker organization controlled by the DPRK's intelligence service. In just one instance in March 2022, Lazarus stole almost $620 million in cryptocurrency.

The indictment alleged that Wu and Cheng used four unnamed Hong Kong front companies to make

payments for goods in U.S. dollars on behalf of the North Korean government. Their North Korean government contact would then arrange the transfer of Bitcoin into a virtual wallet to pay for the goods and compensate Wu and Cheng.[227]

Sale of Cargo Vessels to North Korea via Hong Kong Companies

In the March 2023 Committee report, the panel revealed several instances of cargo vessels being sold to North Korea by Hong Kong shell companies. The ships were then likely used to transport illicit goods.

According to the Committee report, Hong Kong company Sino Ever Treasure Ltd. was the last known foreign shipowner and operator of the ship *SF Bloom*, which then showed up under a North Korean flag. The company, the report said, is a shell entity with a single ship registered to its name, and no online footprint.[228]

Two North Korea-flagged ships, the *Tomi Haru* and *Toyo Haru*, were managed by Hongkong Yong Xiang Shipping Ltd before their acquisition by North Korea. Its director was a Chinese national, Gao HB. Previously, the *Tomi Haru* had been owned by a different Hong Kong company, Sunny International Shipping Co Ltd., which had named it the *Lucky Star 9*. Under this name, the ship visited North Korea ports in 2014 and 2015.[229]

In a third case, the Committee presented evidence that Chinese national Wei TT, the director of Hong Kong company Li Quan Shipping Co. Ltd., sold the vessel *Petrel 8* and several other vessels to North Korea.[230]

Other Notable Hong Kong Companies in UNSC Reports

The three cases above are just a sampling of the dozens of Hong Kong-related incidents documented in the years of UNSC Committee reports. Other cases include:

- In the September 2022 report,[231] four Hong Kong companies were linked to the oil tankers *Heng Xing* and *Joffa*, which were accused of conducting ship-to-ship transfers of oil with North Korean fishing vessels. Hong Kong company Hong Yao International Trading, reportedly owned by Chinese national Liu Zebang, was suspected of arranging the fishing boats to pick up the oil. Heng Cheng Rong (Hong Kong) Marine Co Ltd. was said to own the *Heng Xing*, which was seen in March 2022 off North Korea's coast. A third Hong Kong company, Joffa Trade International, was said to own the *Joffa* tanker, which transferred oil to the *New Konk* (in yet another appearance of this vessel in the Committee reports). *Both* Hong Yao and Heng Chen Rong apparently used the same Hong Kong secretarial services company, Galaxy Company Secretarial Services.

- The September 2023 Committee report] revealed an investigation into the company Hongkong Great Star Development Ltd, or HKGSD, which the report asserted was the registered owner of two vessels that were later transferred to North Korea where they now sail under the North Korean flag.[232] Additionally, HKGSD was reported to be the registered owner and ship manager of the *Shundlli*, which transshipped oil multiple times between December 2022 and June 2023. The Shundlli also apparently geo-spoofed its location along with several other ships (including *New Konk*), in an apparent multi-ship effort to confuse ship trackers.[233]

- The March 2020 report included details on the *Tianyou*, which made at least four port calls in 2019 at Namo, North Korea, to deliver refined petroleum, as well as several ship-to-ship transfers with DPRK vessels.[234] The *Tianyou,* according to the report, was owned by Tian You Shipping Limited, a Hong Kong company, and managed by a Singapore company. The Committee reported that the Singapore company apparently spoke to UNSC investigators, revealing that after the *Tianyou* had repeatedly been observed turning off its automatic identification system in August 2018 (a common tactic for ships that do not want to be tracked), it sent a letter to the Hong Kong ship owner's representative, surnamed Jiang, in which they terminated the management arrangement. This same report noted at least six additional Hong Kong companies that owned six separate vessels known to have conducted illicit trade with North Korea.

The March 2020 report also noted that a Hong Kong art gallery, Tsi Ya Chai on Queens Road in the Central district, had held an exhibition of art from a sanctioned North Korean organization, the Mansudae Art Studio. [235] The studio responded to the Committee's investigators that they merely displayed the art and did not purchase it. Even if true, however, connecting potential buyers via an exhibition may violate the U.N. sanctions.

In short, Hong Kong companies, locations, and individuals appear throughout most of the UNSC North Korea Committee reports over the past two decades. These reports lead to an inescapable conclusion: That Hong Kong and its government's lax sanctions enforcement have made it the world's most critical hub for North Korean sanctions evasion activities, money laundering, and theft.

The Ship "Owner" Who Didn't Know He Owned a Ship

The *Wall Street Journal* reported in 2018[236] on the case of the vessel *Xin Yuan 18*, which had been spotted by Japanese military aircraft alongside a sanctioned North Korean vessel. The report revealed some of the key methods North Korea uses to evade sanctions via Hong Kong's lax corporate systems, with multiple companies and agents, along with fake documentation, involved in concealing the origins of this one vessel.

Xin Yuan 18 was owned by a Hong Kong company, Ha Fa Trade International Co. Ltd. A reporter visited Ha Fa's registered address in Wan Chai, Hong Kong, where they found a secretarial services agency, Yirenjiaren Registration Secretary Ltd. A representative for the agency in its Mainland China headquarters office told the *Journal* that Ha Fa was a client of a different agency that used the same Hong Kong office, Fei Long International Business Co. Ltd. A representative for that agency told the *Journal* that it had registered Ha Fa on behalf of yet another secretarial services agent.

Ha Fa's corporate records from the Companies Registry listed only one director and shareholder, Tang Yun Hui, with the company's business address (which is separate from the registered address) listed in a small village in Hubei Province, China. A *Journal* reporter visited the address, finding a two-story house that was empty, with broken glass in the yard. A neighbor, however, provided a phone number for Tang Yun Hui.

When the *Journal* reached Tang on the phone, he expressed surprise at being listed as the owner of a vessel. It turned out that he was a mere sailor earning less than US$10,000 per year. He confirmed to the *Journal* that the Chinese ID card number in Ha Fa's corporate files was his but noted that he had lost his wallet leaving a ship in 2016 and outside of that incident had frequently turned over his ID to other sailors for paperwork.

This investigation highlighted a remarkable laxity in Hong Kong's Corporate Registry requirements, in which little verification is conducted on the information provided. The result is a system that can be easily exploited by those seeking to evade sanctions while concealing ownership.

A month after the *Wall Street Journal* report, a Companies Registry notice appeared in Ha Fa's corporate files. It said that "Striking the name of [Ha Fa] off the Companies Register is under consideration."[237] The company was struck off several months later.[238]

While at first glance it would appear that the Companies Registry acted in response to the report, that does not appear to be the case: The notice referenced Companies Ordinance section 744, which permits the Companies Registrar to strike off a company if they have "reasonable cause to believe that a company is not in operation or carrying on a business." The source of this "reasonable cause" is unclear, but it is possible that those who ultimately controlled Ha Fa gave notice to the Companies Registry that they were ceasing operation. After all, why continue with a company that has appeared in a global newspaper when one can simply terminate that company and start a new one the next day?

New Findings and Analysis from Open-Source Data

Further investigation into laundered vessel F Lonline's Hong Kong ownership

As noted above, the UNSC North Korea Committee reported in its March 2022 report that a ship known then as *F Lonline* was implicated in vessel identity laundering. According to the report, *F Lonline* was not a real vessel—it was a new name for the *Smooth Sea 3*, which had never actually been transferred with its name but rather had been rebranded as a "newly built" ship, the *Smooth Sea 30*. With this laundering complete, the *F Lonline* could be assigned to vessels at will, such as the *New Konk*, to carry out illicit activities for North Korean interests.

The laundered identity *Smooth Sea 3* was, according to the Committee report, owned by Thailand company Smooth Sea Co. Ltd., followed by Rui He HK Marine Co. Ltd. from June to July 2019. Cheng Xin Shipping Limited owned it from July to October 2019 and renamed it *F Lonline* in October 2019. Finally, Brilliant Trade International Co., Ltd., owned the ship from October 2019.[239]

We took a closer look at one of the Hong Kong shell companies involved in this process, Cheng Xin Shipping Limited, which appeared to essentially purchase, rename, and then resell the vessel, to try to understand how Hong Kong's corporate system had been used to advance North Korea's interests.

Cheng Xin Shipping Limited was formed in September 2016 [240] and dissolved by deregistration in October 2022.[241] It last filed an Annual Return in September 2021.[242] In its initial incorporation form, it listed only one owner, Loo Kiang Khung, based in Singapore.[243] The company used a corporate services company, Smart Team Secretarial Limited, as its secretary and registered address. By the time of its final annual return in 2021, Loo remained the sole shareholder and director.[244]

After the UNSC Committee published its March 2022 report naming Cheng Xin Shipping, the company quickly wound up. On May 16, 2022, the company (via its secretary Startupr CS Limited) applied to deregister itself. [245] This began the process towards ceasing operation.

On June 22, 2022, the company's auditor, Grand Concept Certified Public Accountants, submitted its resignation along with a letter to the Cheng Xin board of directors (of whom there was only one, Loo Kiang Khung). The letter was then filed with the Companies Registry. It stated that "we, as auditors, encountered difficulties on understanding the business substances of the Company."[246]

Also on June 22, the company secretary, Startupr CS Limited, submitted its own resignation.[247]

Loo Kiang Khung is somewhat of a mystery. He holds no other directorships. He does not appear under that name in any social media profiles, nor does he appear in any litigation in Hong Kong or otherwise. The Hong Kong government appears to have taken no action against him.

The only piece of identifying information associated with Loo in the corporate records is his residential address in the incorporation form. There, he lists a Singapore address in Leungkong Tiga.[248] According to Singapore land records, this residential apartment is owned jointly by Lim Ah Moi and Loo Sew Hock. Loo Sew Hock is listed as a citizen of Malaysia.[249]

The above records show that every legitimate company and person associated with Cheng Xin Shipping resigned after the company was named as a sanctions evader. Yet, the Hong Kong government still appears to have taken no action itself against the company or its owner, Loo, despite its purported obligation to enforce North Korea sanctions. Instead, the company was permitted to deregister on its own accord, with final action taken on October 7, 2022.

The Lighthouse Winmore and Hong Kong Government's Inaction

On Dec. 29, 2017, global media reported that the Hong Kong-flagged tanker *Lighthouse Winmore* had been seized by South Korea after transferring marine diesel to the North Korean-flagged tanker *Sam Jong*.[250] According to these reports, upon return to port in South Korea after the transfer, the government had detained the *Lighthouse Winmore* for investigation on Nov. 24, 2017.[251] In the March 2018 UNSC Committee report, the panel revealed how the incident had been discovered: In the days before and after the transfer, *Lighthouse Winmore* had turned off its Automatic Identification System (AIS) to prevent tracking, but the transfer was photographed by an unnamed U.N. member state.[252]

◂ *The Lighthouse Winmore (MarineTraffic).*

▾ *Lighthouse Winmore ship-to-ship transfer with Sam Jong (UNSC North Korea Sanctions Committee).*

At the time, according to the Committee report, the registered owner of *Lighthouse Winmore* was Hong Kong company Win More Shipping Ltd. (**"Win More"**), and the registered operator was another Hong Kong company, Lighthouse Ship Management Ltd (**"Lighthouse"**). On Dec. 30, 2017, online outlet Chinese Daily reported that Win More and Lighthouse share a director, Gong Ruiqiang (龔銳強), a Guangzhou native active in the Southeast Asia shipping business.[253]

On Jan. 4, 2018, SCMP reported that Lighthouse denied knowledge of the *Lighthouse Winmore*'s activities, saying that the vessel had been chartered.[254] The same article noted that Taiwan had released a man on bail, Chen Shih-hsien, who it believed was the oil dealer responsible for the transfer.

After these articles, it appears from corporate and judicial records that there was significant fallout for these companies involving the Hong Kong government—but not due to any action to enforce the U.N. sanctions.

In the first sign of trouble for the company, after the company secretary, Universal Link Consultants Ltd., resigned in the wake of the seizure on Dec. 31, 2017,[255] the Companies Registry issued a notice on Jan. 9 that it may strike Win More off the registry.[256] The notice cited only S.744 of the Companies Ordinance relating to inactive companies, so was likely triggered not by the sanctions violation but by the secretary's resignation. To remedy the issue, Win More appointed a new company secretary, Hong Kong Wellfaith Business Service Int'l Limited, on Jan. 24.[257] On Jan. 30, the Companies Registry issued a notice that it was discontinuing the striking off process.[258]

The companies soon faced a more serious obstacle, however. On Jan. 4, 2018, Bureau Veritas Marine China Co Ltd. (**"BV"**), a Shanghai-based issuer of operating certificates for vessels, wrote to Lighthouse informing them that the class of the vessel and its statutory certificates would be canceled in 30 days, preventing it from operating, according to Win More in a subsequently filed lawsuit.[259] According to Win More in the suit, BV informed them that it was worried about the "stigma to BV caused by the detention of the vessel arising from a suspected violation of the [UNSC] Resolution and the negative impact on its share price and market value as a result thereof."[260] On Feb. 5, according to court filings, BV followed through and canceled *Lighthouse Winmore*'s class and statutory certificates.[261]

Due to this action by BV—and not, it should be noted, due to the North Korea sanctions violation prohibited by Hong Kong law—the Hong Kong Marine Department informed Lighthouse on Feb. 6, and again on May 24, that they would close the vessel's registration unless action was taken within 90 days to resolve the matter.[262]

On May 29, the South Korean Ministry of Oceans and Fisheries informed Lighthouse that for the ship to be released from impoundment, "the flag state (Hong Kong) will have to submit to the Committee plans to prevent the recurrence of such incident, and request that the said vessel be no longer impounded."[263] In response, Lighthouse submitted proposed measures to the Hong Kong Marine Department to prevent further violations and asked the department to make the necessary request to the UNSC Committee for the vessel to be released.[264]

While the Marine Department was reviewing the request, Lighthouse filed an application for judicial review in Hong Kong High Court, requesting that the Director of Marine be ordered to submit the proposed measures to the UNSC.[265] As that matter was pending, the Marine Department submitted the proposed measures to the China Ministry of Foreign Affairs, but wrote that they "are superficial in general," and "lack specific details and are impracticable." The director therefore recommended not submitting the proposed measures.[266]

Finally, on May 2, 2019, Judge Anderson Chow of the High Court rejected Win More's request for an order compelling the Director of Marine to act.[267] On Aug. 28, 2020, the Companies Registry published a notice that Lighthouse would be struck off the Corporate Registry after three months due to not having a secretary or director, both of whom had resigned.[268] Win More, however, remains active as of 2024, though Gong Ruiqiang is no longer the owner, having apparently transferred ownership to Yu Xianhong.[269]

The *Lighthouse Winmore* reportedly was released from impoundment in July 2019 after South Korea requested permission from the UNSC's Sanctions Committee to release it and the committee confirmed that appropriate measures had been taken to prevent the recurrence of sanctions violations.[270] In September 2019, according to publicly available marine traffic records, the ship assumed the name *Jian An 81* under the ownership of another Hong Kong company, LinkedHope International Ltd. By March 2020, it was flying a Panamanian flag rather than a Hong Kong flag.[271]

In January 2022, the ship's name changed to the *Ling Yu* and it was re-flagged to China. The same month, a PRC entity, Yangpu Lingyu International, became the registered owner.[272] There has been no apparent suspicious activity with the vessel since 2019, such as going dark, making port calls in sanctioned countries, or doing ship-to-ship transfers.[273]

Despite claims from Lighthouse and Winmore to the contrary, it is difficult to believe that the owner and manager had no knowledge—or at least suspicion—of the illicit activities being undertaken. According to the High Court ruling, the charter to Chen was a time charter for a fixed period of 12 months.[274] Ordinarily, the owner provides the crew for a time charter, not the charterer.[275] If so, Lighthouse's own crew would have been manning the vessel during any alleged illicit transfer. Additionally, the course a ship takes is public information, and the owner would have easily been able to determine that the vessel's AIS System had been deactivated for a period of days—a strong indication of illicit activity.

As such, it is telling that despite the Hong Kong government having significant involvement in dealing with the fallout of the illicit transfer, including handling Lighthouse's (seemingly voluntary) deregistration and the Marine Department's involvement in litigation related to release of the vessel, no enforcement action appears to have been taken against Lighthouse, Win More, Gong Ruiqiang, or anyone else involved in the alleged illicit transfer. This stands in contrast to Taiwan, where the government launched an immediate investigation into Chen and, a year later in January 2018, sanctioned Chen and his related firms, freezing their assets and forbidding them to do business with banks and other companies.[276]

In issuing the sanctions, the Taiwanese government issued a statement saying, "We share the international responsibility towards regional security, and we cannot tolerate any provocation to international security."[277]

Apparently, the Hong Kong government did not share this view.

Part III: Analysis and Recommendations

Shortcomings in Current Enforcement Schemes

The Limits of Current U.S. Sanctions Enforcement against Hong Kong Companies for Russia Trade

As discussed in this report, since the February 2022 Ukraine invasion, the U.S. has issued several rounds of sanctions targeting companies involved in transshipping of high priority dual-use goods to Russia, including several dozen Hong Kong companies. In most of these cases, the goods involved were electronics with military uses such as semiconductors and other microelectronics.[278] However, this handful of companies constitutes only a tiny fraction of Hong Kong companies and individuals involved in transshipment of Western technology to Russia.

In June 2023, Treasury officials met with banks in Hong Kong to urge them to crack down on transshipments of dual use goods.[279] HSBC, Standard Chartered, Bank of China, HKMA, and ACAMS attended. A list of 38 "high priority dual-use goods" was shared with participants. It is unclear to what extent banks tightened their policies after this meeting, but in September 2023, HSBC halted remittances to and from Russia and Belarus.[280]

In December 2023, the U.S. President issued Executive Order 14114 authorizing secondary sanctions against banks and companies involved in financing companies that ship prohibited goods to Russia.[281] The next month, Treasury officials again visited Hong Kong to hold a meeting with banks. This time, far more attended. Nikkei reported that among those present were executives from Bank of China, ICBC, Bank of Communications, CMB Wing Lung, UBS, Citi, JPM, Goldman, Morgan Stanley, Deutsche, Barclays, and BlackRock.[282] As with the first meeting, it is unclear to what extent the banks have tightened their diligence policies or otherwise changed their behavior since the executive order and meeting.

OFAC finally made use of this new secondary sanctions authority on June 12, 2024, when it announced it had added four individuals and 20 Hong Kong trading companies to the sanctions list under the secondary sanctions executive order.[283] Still, no banks were sanctioned despite the critical nature of bank financing to sanctions evasion activities. A Treasury Department press release[284] noted that the new sanctions were intended to "ratchet up the risk of secondary sanctions for foreign financial institutions that deal with Russia's war economy"— odd phrasing given that no banks were in fact sanctioned, but likely intended to signal that noncompliant banks would be next on the target list. The announcement also included an "updated guidance for foreign financial institutions" on complying with U.S. sanctions and the dangers of not doing so.[285]

Ultimately, however, the bottom line is that U.S. and allied efforts have been inadequate to halt the flow of prohibited western goods from Hong Kong to Russia. Without targeting trade finance, as well as the individuals behind sanctions evading companies and the corporate services and shipping firms that facilitate their trade, the effort is largely a game of whack-a-mole, in which the U.S. will sanction a company or add it to the Entity List, and the owners will then start a new company that is not sanctioned. Hong Kong is a popular location for basing these operations not just because it is relatively politically friendly to Russia, but because creating and replacing corporate identities is very easy to do and difficult to track.

The path from a company being publicly identified as a sanctions evader to that company being added to the sanctions list also moves far too slowly. There is currently no unified process within OFAC, BIS, and the State Department to investigate and establish evidence against sanctions evaders, and not enough staff and resources assigned to the task. In a world where companies can be set up overnight and trade channels established almost as quickly, speed is essential in any sanctions or enforcement response.

To give an example of the timetable involved, in August 2022, in its first of two reports on transshipments of Western goods to Russia, British think tank RUSI reported that the owners of a company that the U.S. government has already added to the Entity List, Sinno Electronics Co Ltd., controlled another company, Sigma Technology Limited, which had been shipping vastly more goods to Russia than Sinno.[286] Despite the publication of this report, it took until February 2024—almost two years later—for Sigma Technology Limited to be added to the U.S. Entity List. To date, it has not been added to any E.U. sanctions lists.[287]

There is a pressing need for the U.S. Congress to pass legislation creating a centralized cross-departmental body to coordinate sanctions and export control investigations, designations, and enforcement. Any such body should also be provided with vastly more staffing, technology, and resources than are currently dedicated to this work. Taking these steps would enable more robust and faster moving investigations, with the goal of rapidly responding to developments as sanctions evaders adapt and regroup by quickly establishing the necessary evidence of illicit conduct and issuing restrictions against both the companies and individuals involved.

Corporate Due Diligence Limitations

While criminal liability for sanctions and export control violations requires willful intent, OFAC and BIS can issue civil penalties based on strict liability.[288] This means that a company or individual that violates sanctions or export control restrictions by conducting prohibited transactions can be subject to steep fines, irrespective of whether they knew about the violations.

U.S. exporters have often relied on their lack of knowledge of reshipments and other prohibited transactions as a defense, despite the strict liability standard. In response to the Bloomberg/C4ADS investigation in 2023, Texas Instruments said that it "strongly opposes our chips' use in Russian military equipment and the illicit diversion of our products to Russia," but claimed "no knowledge" of the onward shipments. Analog Devices similarly said that these reshipments were a "direct violation of our policy," but declined to state what they had done to prevent it.[289]

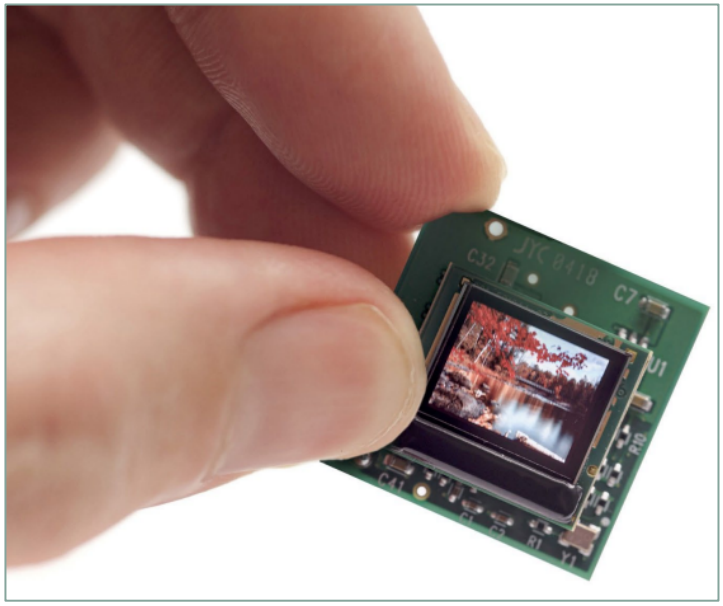
Both OFAC and BIS provide detailed guidance for companies on the due diligence they are legally required to conduct. For export controls, BIS emphasizes the importance of a robust "Know Your Customer" program. Exporters are required to evaluate transactions for any "Red Flags" that suggest the export may be destined for inappropriate end-use, end-user, or destination. These red flags include inconsistencies in the transaction, such as unusual requests or reluctance from the customer to provide end-use information. If red flags are present, exporters must conduct due diligence to investigate and resolve any concerns before proceeding.[290]

OFAC strongly encourages organizations to adopt a risk-based approach by developing a comprehensive sanctions compliance program (SCP). An effective SCP should include management commitment, ensuring senior leadership supports and resources the compliance program; a thorough risk assessment to identify and address potential sanctions risks; internal

controls to prevent and detect prohibited transactions; regular testing and auditing to identify and rectify compliance gaps; and ongoing training for employees to stay updated on compliance requirements.[291]

Nonetheless, the limits of this narrow, risk-based due diligence was exemplified by the *U.S. v. Maxim Marchenko* case discussed above, where a Russian Hong Kong resident was charged with ordering mini-OLED displays (which can be placed in military scopes, among other prohibited uses) from New York-based manufacturer eMagin.[292] When faced with a Hong Kong-based Russian buyer of its sensitive dual-use goods, eMagin asked Marchenko via email to "Please confirm this does not include Russia or Ukraine for end country," to which Marchenko responded, "I confirm that this does not include Russia or Ukraine for end country." As the shipments proceeded, eMagin sent various questions about the end users. Marchenko simply lied, saying that the end user was the National Health Commission in China, which would use the mini-OLEDs for electron microscopes. Eventually, at the advice of law enforcement, eMagin declined to continue the sales and referred Marchenko to a fake undercover company which proceeded to conduct a sting operation. However, by this point many units had already been shipped.

To date, while the U.S. has brought several enforcement actions against overseas evaders of the Russian sanctions program, with respect to American goods producers, it has neither brought any legal actions nor announced any investigations. Ramping up civil enforcement actions when inadequate due diligence programs fail to catch sanctions and export control violations may be necessary to nudge companies towards spending more resources in building out these risk-based processes.



An eMagin OLED microdisplay (eMagin press handout).

Policy Recommendations

Hong Kong's value as a hub for sanctions evasion has grown significantly in recent years. This report underscores the urgent need for comprehensive and decisive measures to stem this trend. While these recommendations are relevant to all democratic nations, most of our recommendations focus on U.S. policy due to the United States' unparalleled influence over the global economy and its demonstrated political will to address these issues.

1 The U.S. should use its secondary sanctions authority to designate Hong Kong and Chinese banks financing illicit trade.

The U.S. government should issue secondary sanctions against Hong Kong and Chinese financial institutions financing or providing services to Hong Kong's sanctions evaders. As described in this report, in Hong Kong the ease and speed with which corporate entities can be created and the ability to mask beneficial owners severely limit the impact of sanctions on trading companies. Financial institutions, however, do not have the same luxury: raising capital, obtaining licenses, and establishing the proper entities requires significantly more time and effort. Only by sanctioning financial institutions involved in financing sanctions evasion can the U.S. genuinely curtail the flow of illicit goods and funds to sanctioned regimes.

In December 2023, the Biden Administration issued Executive Order 14114,[293] which permits secondary sanctions on non-U.S. financial institutions working with Russian sanctioned persons, as well anyone supporting the Russian military-industrial base in any capacity. Since then, the administration has repeatedly threatened to use this power against Hong Kong and Chinese financial institutions,[294] but so far has not done so.

The North Korea and Iran sanctions regimes also permit secondary sanctions on foreign financial institutions facilitating illicit transactions these regimes under Executive Order 13810 (North Korea)[295] and Executive Order 13902 (Iran).[296] The U.S. should make use of this authority with respect to Hong Kong and Chinese foreign financial firms facilitating such illicit transactions.

2 The U.S. should Designate Hong Kong as a Primary Money Laundering Concern ("PMLC").

The U.S. Treasury should designate Hong Kong as a primary money laundering concern under Section 311 of the Patriot Act.[297] This designation allows the Treasury Department (via FinCEN) to pursue special measures against jurisdictions or financial institutions abroad if it determines there are reasonable grounds to conclude the jurisdiction or financial institution is of primary money laundering concern. The special measures range in severity, permitting a more tailored approach to Hong Kong's particular illicit transaction risk than simply sanctioning the jurisdiction or those within it.[298]

The special measures permitted by the law that we recommend taking with respect to Hong Kong are:

- Requiring U.S. financial institutions dealing with Hong Kong to maintain records and report to the FinCEN information about transactions within Hong Kong or with Hong Kong persons;
- Requiring U.S. financial institutions to obtain and retain information concerning the beneficial ownership of any account opened or maintained by a Hong Kong person in the United States;

Requiring U.S. banks that open payable-through or correspondent accounts for foreign financial institutions to identify and obtain information on each customer permitted to use or whose transactions are routed through the payable-through or correspondent account.

In particular, the requirement for additional disclosures in correspondent accounts would have a significant impact on sanctions evasion activities in Hong Kong. It would effectively cut off many avenues for financing illicit Hong Kong trade using the U.S. dollar, significantly increasing costs and difficulty for foreign trade firms accustomed to using the world's reserve currency even for illegal transactions.

3 Congress should act to increase resources and coordination across government departments responsible for sanctions and export control enforcement.

To effectively enforce complex sanctions and export control regimes, the US should significantly increase funding for additional resources and personnel to the Commerce, Treasury and State Department offices responsible for investigation and enforcement. Congress has taken incremental steps to increase funding for certain offices within OFAC and BIS.[299] Still, the resources these teams are provided are insufficient to respond and enforce the vast proliferation of sanctions evaders in Hong Kong and elsewhere. Congress should consider authorizing and appropriating more funding for additional enforcement officers within OFAC and BIS, as well as earmarks for data and analytical tools that allow these departments to maintain a responsive export control regime that keeps pace with technological change. Enhanced resources will ensure that these departments have the resources and expertise necessary to conduct thorough investigations and take swift enforcement actions against violators.

As sanctions and export control efforts have become increasingly intertwined, cross-departmental coordination has often been ad hoc and led to confusion. A specialized cross-departmental unit can enhance coordination and streamline efforts across different government agencies. For example, formally establishing and adequately resourcing the Export Enforcement Coordination Center (E2C2) through the Export Controls Enforcement Improvement Act of 2024 would help to unify efforts by consolidating expertise, resources, and information from various departments. Similar measures could be taken with respect to sanctions designations and enforcement to consolidate efforts across departments.[300]

4 The U.S., E.U., and their allies should focus more resources on targeting individuals and supporting entities facilitating sanctions evasion.

Western sanctions programs—most notably and recently the Russia sanctions program—have primarily focused on sanctioning trading companies, with far less attention to the individuals or entities facilitating those companies' activities, including logistics firms, insurers, and corporate registry services providers. In industries and locations where founding and building businesses take significant time and resources (such as financial firms as noted above), this can be effective. But for small trading companies in Hong Kong, the approach is woefully inadequate.

The case of Arttronix—discussed in this report—exemplifies the problem. After Arttronix was sanctioned by the U.S. for supplying UAV parts to Iran, its owner quickly shut down the company. He then founded a new company with a different name and a placeholder owner to conceal his ownership.[301] This process from application to approval by the Hong Kong government took a week, at which point a man whose company had been sanctioned was back in business.

To better disrupt transactions in illicit goods, enforcement agencies should prioritize efforts to target the individuals and entities facilitating the operations of these corporate shells. Acting against a logistics provider involved in shipping large volumes of dual-use items is likely to be more disruptive than designating a handful of small trading firms that can be reconstituted under new names. Furthermore, adding addresses at a high risk of illicit diversion to the Commerce Department's Entity List, as BIS did on June 12, 2024, is a welcomed approach to ensure corporate service providers are not facilitating this trade.

5 Global financial firms should enhance AML procedures to capture data like customs records and suspicious vessel activity.

Banks' Anti-Money Laundering (**"AML"**) processes are designed to detect and prevent illicit financial activities by identifying suspicious behavior. These processes typically involve reviewing public information about clients by monitoring public records, media reports, and other sources for any adverse information that could indicate involvement in illegal or sanctioned activities. AML systems often rely on Know Your Customer (KYC) protocols, transaction monitoring systems, and the screening of clients against various watchlists and databases to identify potential risks.[302]

To further enhance the effectiveness of AML procedures, banks should expand their data collection (or partner with organizations specializing in these data types) to include customs records, vessel suspicious activity data, and other public data currently used by governments and organizations to uncover sanctions-violating companies. By incorporating these additional data sources, banks can gain a more comprehensive view of their clients' activities and identify red flags that may not be evident through traditional financial records alone. Recent advancements in artificial intelligence can facilitate the parsing and analysis of these large data sets, enabling AML teams to efficiently flag potential concerns.

6 The U.S., E.U., and their allies should increase enforcement and penalties against manufacturers and distributors of sensitive technologies.

While agencies made improvements to the scale and scope of enforcement actions in 2023, substantial quantities of sensitive Western-made dual use technology continue to make their way to Russia, Iran, and North Korea through transshipment hubs like Hong Kong.

Western governments should increase enforcement efforts and the severity of penalties against manufacturers, exporters, and distributors who fail to conduct sufficient due diligence and take account of red flags, particularly in the semiconductor and high-technology sectors. This includes imposing strict penalties on companies that knowingly or negligently allow their products to be diverted to sanctioned entities. Greater enforcement activity and increased civil penalties would encourage firms to invest more in compliance and reduce the risk of their goods being used for prohibited purposes. Increasing the costs of inaction is the best way to get companies to take their compliance obligations seriously.

ENDNOTES

[1] While we have relied on C4ADS' data in preparing this report, the conclusions and analysis in the report were developed by us.
[2] "As Russia Completes Transition to a Full War Economy, Treasury Takes Sweeping Aim at Foundational Financial Infrastructure and Access to Third Country Support," U.S. Department of Treasury, June 12, 2024.
[3] For a more comprehensive overview of U.S. Sanctions, *see* "Overview of US sanctions laws and regulations," Norton Rose Fulbright, February 6, 2024.
[4] *See* "Entity List," U.S. Department of Commerce: Bureau of Industry and Security, last modified July 2024.
[5] "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)," The European Parliament and the Council of the European Union, May 20, 2021.
[6] "European Union Sanctions," European Union External Action: The Diplomatic Service of the European Union, October 7, 2023.
[7] "What is the Security Council?" United Nations Security Council.
[8] Boucher, Alix J., and Victoria K. Holt. "*Panels of Experts: Roles and Challenges.*" Targeting Spoilers: The Role of United Nations Panels of Experts. Stimson Center, January 1, 2009.
[9] "*Cap.537 United Nations Sanctions Ordinance*," Hong Kong e-Legislation.
[10] "*Cap.575 United Nations (Anti-Terrorism Measures) Ordinance*," Hong Kong e-Legislation.
[11] "Carrie Lam: Hong Kong's leader says she has to keep piles of cash at home," BBC, November 28, 2020.
[12] "Hong Kong's Lee Sidestepped Sanctions With $1.4 Million in Cash," Bloomberg, July 5, 2022.
[13] "Timeline - EU Sanctions against Russia," European Council: Council of the European Union, last modified June 28, 2024; "Ukraine and Russia Sanctions," U.S. Department of State.
[14] "Commerce Department Announces Expansion of Export Restrictions on Russia," U.S. Department of Commerce: Bureau of Industry and Security, April 28, 2014.
[15] "EU restrictive measures in view of the situation in Eastern Ukraine and the illegal annexation of Crimea," Council of the European Union, July 29, 2014.
[16] "Timeline - EU sanctions against Russia," European Council: Council of the European Union, last modified June 28, 2024; "*A Timeline of All Russia-Related Sanctions*," Radio Free Europe Radio Liberty, September 19, 2018.
[17] "What are the sanctions on Russia and have they affected its economy?" BBC, February 23, 2024.
[18] "*A Guide to US, UK, and EU Sanctions and Export Controls on Russia and Belarus*," Debevoise & Plimpton, December 22, 2023.
[19] "Common High Priority List," U.S. Department of Commerce: Bureau of Industry and Security, last modified February 23, 2024.
[20] Exec. Order No. 14114, "*Taking Additional Steps With Respect to the Russian Federation's Harmful Activities*," *3 C.F.R. 313 (December 22, 2023)*.
[21] *See* Zachary Laub, "International Sanctions on Iran," Council on Foreign Relations, July 15, 2015.
[22] Kali Robinson, "What Is the Iran Nuclear Deal?" Council on Foreign Relations, October 27, 2023.
[23] Ibid.
[24] "Iran: Background and U.S. Policy," Congressional Research Service, April 22, 2024, at 22-24.
[25] "Re-imposition of the sanctions on Iran that had been lifted or waived under the JCPOA," U.S. Department of the Treasury: Office of Foreign Assets Control, November 4, 2018.
[26] "EU sanctions against Iran," European Council: Council of the European Union, June 4, 2024.
[27] "What to Know About Sanctions on North Korea," Council on Foreign Relations, July 27, 2022.
[28] "1718 Sanctions List," U.N. Security Council, last modified July 12, 2024.
[29] "*UN Documents for DPRK (North Korea): Sanctions Committee Documents*," Security Council Report, last modified March 7, 2024. These reports will be discussed in more detail in the North Korea findings section below.
[30] Dr. Aaron Arnold, "*Russia Just Gutted the UN Panel of Experts on North Korea – What Now?*" RUSI, April 3, 2024.
[31] "What to Know About Sanctions on North Korea," Council on Foreign Relations, July 27, 2022.
[32] Ibid.
[33] "EU sanctions against North Korea," European Council: Council of the European Union, June 4, 2024.
[34] "What to Know About Sanctions on North Korea," Council on Foreign Relations, July 27, 2022.
[35] Angela Stent, Yun Sun, and Adrianna Pita, "The dynamics of the Russia-China partnership," Brookings, May 22, 2024.
[36] Emil Avdaliani, "All Smiles in the Russia-Iran Trade Bazaar," CEPA, January 17, 2024.

[37] "North Korea-Russia Relations: Current Developments," Congressional Research Service, May 6, 2024.
[38] Mohamed Zeeshan, "India Turns the Page on Ties with Russia After Ukraine War," The Diplomat, January 3, 2024.
[39] "*REPORT: "Russia Shifting Import Sources Amid U.S. and Allied Export Restrictions*," Silverado, January 22, 2023.
[40] James Byrne et. al, "*Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine*," RUSI, August 2022.
[41] "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," U.S. Department of Justice, March 2, 2023.
[42] "*Effectiveness of U.S. Sanctions Targeting Russian Companies and Individuals*," Free Russia Foundation, January 2023.
[43] "Special report: How U.S.-made chips are flowing into Russia," Nikkei Asia, April 12, 2023.
[44] Gigi Lee and Fong Tak Ho, "Public records map Wagner Group's Hong Kong connections," Radio Free Asia, June 27, 2023.
[45] Nathaniel Taplin, "How Russia Supplies Its War Machine," *Wall Street Journal*, last modified March 10, 2023.
[46] Sheridan Prasso, "Chips From Texas Instruments and Other US Makers Flow Into Russia Despite Ban," Bloomberg, December 21, 2023.
[47] James Pomfret and Clare Jim, "Hong Kong leader says "no legal basis" to act on Russian superyacht," Reuters, October 10, 2022.
[48] Greg Torode and Donny Kwok, "Russian oligarch's luxury yacht departs Hong Kong port," Reuters, October 20, 2022.
[49] Steve Stecklow, David Gauthier-Villars, and Maurice Tamman, "The supply chain that keeps tech flowing to Russia," Reuters, December 13, 2022
[50] "Solutions," Pixel Devices, last modified 2021.
[51] Steve Stecklow, David Gauthier-Villars, and Maurice Tamman, "The supply chain that keeps tech flowing to Russia," Reuters, December 13, 2022.
[52] James Byrne et al., "*The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV*," RUSI, December 2022.
[53] Ibid.
[54] Ibid.
[55] "*Effectiveness of U.S. Sanctions Targeting Russian Companies and Individuals*," Free Russia Foundation, January 2023.
[56] "Special report: How U.S.-made chips are flowing into Russia," Nikkei Asia, April 12, 2023.
[57] Ibid.
[58] Ibid.
[59] Sheridan Prasso, "Chips From Texas Instruments and Other US Makers Flow Into Russia Despite Ban," Bloomberg, December 21, 2023.
[60] "Russian International Money Launderer Arrested for Illicitly Procuring Large Quantities of U.S.-Manufactured Dual-Use Military Grade Microelectronics for Russian Elites," U.S. Department of Justice: Office of Public Affairs, September 18, 2023.
[61] Josh Russell, "*Hong Kong money launderer nabbed in smuggling of military-grade gear to Russia*," Courthouse News Service, last modified September 18, 2023. The Complaint only refers to the company as "Company-1," a mini-OLED producer based in Duchess, New York. eMagin is the only company that fits this description.
[62] Complaint, *U.S. v Maxim Marchenko*, 23-mj-6181 (S.D.N.Y. 2023).
[63] "Russian International Money Launderer Sentenced to Three Years in Prison for Illicitly Procuring Large Quantities of U.S.-Manufactured Dual-Use, Military Grade Microelectronics for Russian Entities," U.S. Department of Justice, July 17, 2024.
[64] "Russia-related Designations; Issuance of Russia-related General License and Frequently Asked Questions; Zimbabwe-related Designation, Removals and Update; Libya-related Designation Update," U.S. Department of Treasury: Office of Foreign Assets Control, September 15, 2022.
[65] Ibid.
[66] "List of Common High Priority Items," European Union: Finance, last modified February 2024; "Common High Priority List," Bureau of Industry and Security, February 23, 2024.
[67] Russian Customs Data: December 2023.
[68] Ibid.
[69] Ibid. Headquarters location data retrieved from Crunchbase.com.
[70] Ibid. Texas Instruments places twelfth in total value despite leading the list of cargoes by number, likely due to its focus on lower cost, mass produced chips and other technology, where companies topping the value list like Intel and Analog Devices focus on higher end, more specialized products.
[71] Headquarters location data retrieved from Crunchbase.com.
[72] "Connecting global markets for your success," Piraclinos Limited, last updated 2024.
[73] "With Wide-Ranging New Sanctions, Treasury Targets Russian Military-Linked Elites and Industrial Base," U.S. Department of Treasury, September 14, 2023.
[74] "Compound Photonics announces the opening of MicroLED Innovation Acceleration Center (MiAC) in Chandler, Arizona," Government of Chandler, Arizona, November 16, 2020.
[75] *See* Snap, Inc., "Spectacles."

[76] KGOnTech, "Exclusive: Snap Buying Compound Photonics," January 7, 2022. The Compound Photonics website no longer exists but was previously located at http://www.compoundphotonics.com. When it was last crawled by the Internet Archive on October 3, 2022, the page redirected to the WaveOptics website at https://waveoptics.ar, which lists Snap Inc. as its owner.
[77] "Meet Our Amazing Team," Piraclinos Limited, last modified 2024.
[78] "Katerina Hadjikyriacou," LinkedIn.
[79] "About Our Company," Treppides, last modified 2024.
[80] For example, the first on the list alphabetically is 4AVS Limited, which appears to run an app to help people "sync with the lunar rhythm and change your life." "Moonlia App," Moonlia.
[81] "Svilen Spasov," LinkedIn.
[82] "Svilen Spasov," Gov.uk.
[83] "Cyprus Registered Companies Affiliations for Similarly Named Officials: (Svilen Spasov)," Cyprus Corporate Registry, last modified 2024.
[84] "IBFS United," IBFS United, last modified 2024.
[85] "IBFS United," IBFS United; archived at Wayback Machine (https://web.archive.org/), captured on February 28, 2024.
[86] "IBFS United," IBFS United, last modified 2024.
[87] "Cyprus," IBFS United, last modified 2024; "Services in Relation to Taxation," IBFS United," last modified 2024.
[88] Director Particulars Search, Symbat Belekova. Hong Kong Companies Registry, *last accessed* May 13, 2024.
[89] Symbat Belkova, Companies House, UK.gov.
[90] "Company Profile," Vectrawave.
[91] Ibid.
[92] Open Sanctions, "AO Trek," last accessed April 15, 2024 (link now dead).
[93] Ibid.
[94] AO Trek appears throughout the December 2023 data, with 125 cargoes from Hong Kong that month worth $2.84m. The Vectrawave cargoes were the highest value, but other Western/U.S. products were shipped in large numbers from companies including Analog Devices, Texas Instruments, and Maxim Integrated Products. The highest value cargoes after Vectrawave came from M/A-Com, Traco Power, and Adlink Technology, all of low weight and likely relatively high-cost products. In some cases, packages that weighed very little still listed high values. For example, a $32,000 cargo of Analog Devices goods on December 3 weighed just 1.64kg. All December shipments to AO Trek came from three consigners: Align Trading Co Limited (9 cargoes), Hytera Communications (104 cargoes), and Mei Xin Electronic HK Co Ltd (9 cargoes).
[95] "Trading," Corp-Link International Logistics Limited."
[96] "Corp Link International Logistics Ltd." Made-in-China, last modified 2024.
[97] Hong Kong Companies Registry search data.
[98] 2023 Annual Return, Corp-Link International Logistics Ltd. Hong Kong Companies Registry, May 5, 2023.
[99] Ibid.
[100] "U.S. Continues to Degrade Russia's Military-Industrial Base and Target Third-Country Support with Nearly 300 New Sanctions," U.S. Department of the Treasury, May 1, 2024.
[101] "*Welcome to DEXP International Limited*," DEXP, last modified 2024.
[102] "Analysis: How Nvidia Surpassed Intel In Annual Revenue And Won The AI Crown," The Channel Co., February 26, 2024.
[103] Don Clark, Ana Swanson, "*U.S. Restricts Sales of Sophisticated Chips to China and Russia*," *New York Times*, August 31, 2022.
[104] "Организация ООО "СТОТЕХНО/ STOTECHNO LLC," List-Org.
[105] 2023 Annual Return, DEXP International Limited, Hong Kong Companies Registry, September 13, 2023.
[106] Kathleen Li, Ellen Wan, Harry McKenny, "Is Hong Kong Serving Russia American Chips?" *Epoch Times*, April 18, 2023.
[107] "Gleb Khitrin," LinkedIn.
[108] *See* 2024 Annual Return, Tsy Global Solutions Limited. Hong Kong Companies Registry, March 23, 2024.
[109] Ibid.
[110] "Assignment of Life Insurance," The Hongkong and Shanghai Banking Corporation Limited and DEXP International Limited. Hong Kong Companies Registry, January 21, 2022.
[111] "Deed of Release," The Hongkong and Shanghai Banking Corporation Limited. Hong Kong Companies Registry, April 25, 2023.
[112] This issue is discussed further in the Recommendations section of this report.
[113] CHPL Dataset, December 2023.
[114] Ibid.
[115] Ibid.
[116] "Treasury Sanctions Impede Russian Access to Battlefield Supplies and Target Revenue Generators," U.S. Department of the Treasury, July 20, 2023.
[117] "О компании/About the Company," Альтрабета/Alterbeta.
[118] "Preferential zone," Chipgoo, last modified 2024.
[119] Incorporation Form, Chipgoo Technology Limited. Hong Kong Companies Registry, March 2, 2024; Incorporation Form, Chipgoo Electronics Limited. Hong Kong Companies Registry, November 22, 2023.
[120] Notice of Change of Company Name, Chipgoo Technology. Hong Kong Companies Registry, October 31, 2023.
[121] 2024 Annual Return, Chipgoo Technology Limited. Hong Kong Companies Registry, March 2, 2024; 2023 Annual Return, Chipgoo Electronics Limited. Hong Kong Companies Registry, November 22, 2023.

[122] Wuxin Lin, "chipgoo is your electronic components supplier," LinkedIn, November 27, 2023.
[123] "Financial Sanctions Notice: Russia," HM Treasury: Office of Financial Sanctions Implementation, May 19, 2023.
[124] "U.S. Treasury Designates Russian State-Owned Sovcomflot, Russia's Largest Shipping Company," U.S. Department of the Treasury, February 23, 2024.
[125] "Authorizing Transactions Involving Certain Sovcomflot Vessels," General License No. 93, Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR Part 587, U.S. Department of the Treasury: Office of Foreign Assets Control, February 23, 2024.
[126] Julian Lee and Alex Longley, "Russia's Sovcomflot Is Renaming Oil Tankers Hit by US Sanctions," Bloomberg, April 30, 2024.
[127] 2023 Annual Return, Albatross Marine Asia Limited. Hong Kong Companies Registry, July 17, 2023; 2023 Annual Return, AM Asia M6 Limited. Hong Kong Companies Registry, July 24, 2023.
[128] General Details, Albatross Marine Asia Limited. Hong Kong Companies Registry, July 17, 2023; General Details, AM Asia M6 Limited. Hong Kong Companies Registry, July 17, 2024.
[129] Alejandro Gonzalez, "US Sanctions target Russia's state-backed leasing companies," Leasing Life, March 7, 2022.
[130] "From Crimea to Iran: Two More Ships Join Russia's Grain-Smuggling Fleet," Bellingcat, April 23, 2024.
[131] "У россии возникли проблемы с проходом некоторых судов через Босфор, сообщает мониторинговая группа," Крымского ветра (Crimean Wind), Telegram, March 3, 2024.
[132] *See* "Agriculture Weaponised: The Illegal Seizure and Extraction of Ukranian Grain by Russia," Global Rights Compliance, November 2023.
[133] *See, e.g.,* "Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime," U.S. Department of the Treasury, March 9, 2023.
[134] "Hacked Documents Reveal Iran's Strategies To Bypass Sanctions," Iran International, February 13, 2024.
[135] Elisabeth Braw, "Russia's growing dark fleet: Risks for the global maritime order," Atlantic Council, January 11, 2024; Katherine Camberg, "Ghose Ships Already wreak Havoc," Center for Maritime Strategy, November 28, 2023.
[136] Danny Citrinowicz, "Iran is on its way to replacing Russia as a leading arms exporter. The US needs a strategy to counter this trend," Atlantic Council, February 2, 2024.
[137] *See* "Treasury Sanctions Transnational Procurement Network Supporting Iran's Ballistic Missile and UAV Programs," U.S. Department of the Treasury, February 2, 2024. (Hong Kong companies involved in procuring UAV parts); "Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime," U.S. Department of the Treasury, March 9, 2023. (Hong Kong front companies receiving proceeds of Iranian petrochemical sales).
[138] *See, e.g.,* "Treasury Targets Companies and Vessels Facilitating Qods Force and Houthi Commodity Shipments," U.S. Department of the Treasury, March 6, 2024.
[139] "Huawei CFO Wanzhou Meng Admits to Misleading Global Financial Institution," U.S. Department of Justice: Office of Public Affairs," September 24, 2021 (Meng's admissions and Deferred Prosecution Agreement announcement).
[140] "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud," U.S. Department of Justice: Office of Public Affairs, January 28, 2019. (DOJ charges announcement).
[141] Ibid.
[142] Ibid
[143] Ian Talley, "How Iran Tapped International Banks to Keep Its Economy Afloat," *Wall Street Journal*, June 22, 2022.
[144] Ibid.
[145] "Treasury Targets International Networks Supporting Iran's Petrochemical and Petroleum Industries," U.S Department of the Treasury, January 23, 2020.
[146] "Triliance Petrochemical Co. Ltd.," Open Sanctions.
[147] "Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime," U.S. Department of the Treasury, March 9, 2023.
[148] "Treasury Sanctions Procurement Network Supporting Iran's One-Way Attack UAV Program," U.S. Department of the Treasury, September 27, 2023.
[149] Ibid.
[150] "Addition of Entities and Revision to Existing Entities on the Entity List; Removal of Existing Entity from the Military End User List," Department of Commerce: Bureau of Industry and Security, September 27, 2023.
[151] 2023 Annual Return, Sunrising Logistics. Hong Kong Companies Registry, October 16, 2023.
[152] "Treasury Sanctions Transnational Procurement Network Supporting Iran's Ballistic Missile and UAV Programs," U.S. Department of the Treasury, February 2, 2024.
[153] "Treasury and the United Kingdom Target Qods Force Deputy Commander and Houthi-Affiliated Supporters," U.S. Department of the Treasury, February 27, 2024.
[154] "Treasury Targets Companies and Vessels Facilitating Qods Force and Houthi Commodity Shipments," U.S. Department of the Treasury, March 6, 2024.
[155] Ibid.
[156] "DOJ Unseals Charges Against Iranian and Chinese Nationals for Procurement Fraud Involving the Acquisition of Components for Drones on Behalf of the Iranian Government," United States Attorney's Office: District of Columbia, December 19, 2023.

[157] "Justice Department Announces Terrorism and Sanctions-Evasion Charges and Seizures Linked to Illicit, Billion-Dollar Global Oil Trafficking Network That Finances Iran's Islamic Revolutionary Guard Corps and Its Malign Activities," U.S. Department of Justice: Office of Public Affairs, February 2, 2024.
[158] Ibid.
[159] "Chinese Nationals Charged with Illegally Exporting U.S.-Origin Electronic Components to Iran and Iranian Military Affiliates," U.S. Department of Justice: Office of Public Affairs, January 31, 2024.
[160] "Iranian National Charged With Illegally Exporting Electrical Equipment to Iran," United States Attorney's Office: District of Columbia, March 9, 2023.
[161] "Treasury Sanctions Procurement Network Supporting Iran's UAV and Military Programs," U.S. Department of the Treasury, April 19, 2023.
[162] These companies are discussed further in the independent investigation findings section below.
[163] "Criminal Complaint by Telephone or Other Reliable Electronic Means," United States District Court for the Central District of California, October 16, 2020.
[164] *See* Daniel E. Mouton, "Iranian drones have proliferated under US watch," Atlantic Council, April 2, 2024.
[165] Uzi Rubin, "*Russia's Iranian-Made UAVs: A Technical Profile*," RUSI, January 13, 2023.
[166] "Dissecting Iranian drones employed by Russia in Ukraine," Ukraine Field Dispatch, November 2022.
[167] "Treasury Sanctions Procurement Network Supporting Iran's UAV and Military Programs," U.S. Department of the Treasury, April 19, 2023.
[168] "Iranian National Charged With Illegally Exporting Electrical Equipment to Iran," United States Attorney's Office: District of Columbia, March 9, 2023.
[169] "2022 Annual Return," Arttronix International (HK) Limited. Hong Kong Companies Registry, November 9, 2022.
[170] Notice of Resignation of Company Secretary and Director, Arttronix International (HK) Limited. Hong Kong Companies Registry, April 21, 2023.
[171] 《閉會通過的特別決議，偉電國際（香港）有限公司》, Hong Kong Companies Registry, April 26, 2023.
[172] Application for Deregistration of Private Company or Company Limited by Guarantee, Arttronix International (HK) Limited, Hong Kong Companies Registry, February 1, 2024 (attaching notice from Inland Revenue Department stating no objection to deregistration after receiving the request on April 28, 2023—days after the U.S. announcement).
[173] Ibid.
[174] Incorporation Form, ETS International (HK) Limited. Hong Kong Companies Registry, April 24, 2024.
[175] Ibid.
[176] Ibid.
[177] Hong Kong Companies Registry search data.
[178] "Treasury Sanctions Transnational Procurement Network Supporting Iran's One-Way Attack UAV Program," U.S. Department of the Treasury, September 27, 2023,
[179] Hong Kong Companies Registry search data.
[180] 2023 Annual Return, Hongkong Himark Electron Model Limited. Hong Kong Companies Registry, September 13, 2023.
[181] Ibid.
[182] Incorporation Form, Hongkong Himark Electron Model Limited. Hong Kong Companies Registry, September 7, 2017.
[183] Notice of Resignation of Company Secretary and Director, Hongkong Himark Electronic Model Limited. Hong Kong Companies Registry, November 8, 2023.
[184] Hong Kong Companies Registry search data.
[185] Ibid.
[186] Ibid.
[187] Ibid.
[188] "Sahara Thunder," WikiIran.
[189] Ibid.
[190] Ibid.
[191] See 2023 Annual Return, HK Petroleum Enterprises Cooperation. Hong Kong Companies Registry, July 15, 2023; 2023 Annual Return, HK Shipping Cooperation Limited. Hong Kong Companies Registry, December 22, 2023; Articles of Association, HK Shipping Cooperation Limited. Hong Kong Companies Registry, December 22, 2021.
[192] Ani Sz's LinkedIn Profile, LinkedIn.
[193] Ali Jef's LinkedIn Post, LinkedIn.
[194] 2023 Annual Return, HK Petroleum Enterprises Cooperation. Hong Kong Companies Registry, July 15, 2023; 2023 Annual Return, HK Shipping Cooperation Limited. Hong Kong Companies Registry, December 22, 2023.
[195] Incorporation Form, HK Energy Corporation Limited. Hong Kong Companies Registry, January 29, 2024.
[196] Incorporation Form, Orient Source (HK) Limited. Hong Kong Companies Registry, August 26, 2014.
[197] Orient-Source (HK) Limited's website.
[198] Incorporation Form, Orient Source (HK) Limited. Hong Kong Companies Registry, August 26, 2014.
[199] "Alistair Jeffries," X, February 18, 2013.
[200] 2023 Annual Return, Orient Source (HK) Limited. Hong Kong Companies Registry. August 26, 2023.
[201] Elizabeth Rosenberg and Neil Bhatiya, "Busting North Korea's Sanctions Evasion," Center for a New American Strategy, March 4, 2020.
[202] King Mallory, "*North Korean Sanctions Evasion Techniques*," RAND, September 23, 2021.
[203] Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," Wired, May 17, 2016.

[204] Elizabeth Rosenberg and Neil Bhatiya, "Busting North Korea's Sanctions Evasion," Center for a New American Strategy, March 4, 2020.
[205] "*United Nations Sanctions (Democratic People's Republic of Korea) Regulation*," Hong Kong e-Legislation, June 15, 2007.
[206] "List of individuals and entities published under section 31 of the United Nations Sanctions (Democratic People's Republic of Korea) Regulation," The Government of the Hong Kong Special Administrative Region of the People's Republic of China: Commerce and Economic Development Bureau, March 9, 2024. (North Korea sanctioned persons); "List of relevant ships published under section 31A of the United Nations Sanctions (Democratic People's Republic of Korea) Regulation," The Government of the Hong Kong Special Administrative Region of the People's Republic of China: Commerce and Economic Development Bureau, June 22, 2018. (North Korea sanctioned vessels).
[207] U.N. Security Council, "1718 Sanctions List." (United Nations sanctions under Security Council res. 1718)
[208] According to a review of the U.S. SDN list at "Sanctions List Search," U.S. Department of the Treasury: Office of Foreign Assets Control, filtered by DPRK programs and locations.
[209] According to a review of the U.S. SDN list at Sanctions List Search, filtered by DPRK programs and locations.
[210] "Leader (Hong Kong) International," United Nations Security Council.
[211] U.N. Security Council, "1718 Sanctions List." (United Nations sanctions under Security Council res. 1718).
[212] Hong Kong Companies Registry search data; *see also* 2011 Annual Return, Leader (Hong Kong) International Trading Limited. Hong Kong Companies Registry, October 18, 2011; 2012 Annual Return, Leader (Hong Kong) International Trading Limited. Hong Kong Companies Registry, October 18, 2012.
[213] S.744, Leader (Hong Kong) International Trading Limited. Hong Kong Companies Registry, April 22, 2016; S.746, Leader (Hong Kong) International Trading Limited. Hong Kong Companies Registry, August 26, 2016; *See also* Hong Kong Companies Ordinance, "*Part 15, Dissolution by Striking off or Deregistration, Division 1 – Striking Off*," Hong Kong e-Legislation, last modified July 1, 2024.
[214] Search conducted at https://legalref.judiciary.hk/lrs/common/ju/judgment.jsp.
[215] Technically a midterm report every March and a final report every September. *See* "Reports," United Nations Security Council, last modified March 7, 2024.
[216] "March 2020 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 2, 2020, at 19.
[217] Ibid.
[218] "August 2020 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, August 28, 2020, at 12.
[219] Christoph Koettl, "*How Illicit Oil Is Smuggled Into North Korea With China's Help*," *New York Times*, March 24, 2021.
[220] "March 2021 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 4, 2021.
[221] *Brilliant Trade International, Co., Limited, Company Name Search*, Hong Kong Companies Registry, *last accessed* March 19, 2024.
[222] "March 2022 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 1, 2022.
[223] "September 2021 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, September 8, 2021.
[224] "September 2023 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, September 12, 2023.
[225] "September 2023 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, September 12, 2023, at 56.
[226] "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," U.S. Department of the Treasury, April 24, 2023; "North Korean Foreign Trade Bank Rep Charged for Role in Two Crypto Laundering Conspiracies," United States Attorney's Office: District of Columbia, April 24, 2023.
[227] *Indictment, U.S. v. Sim Hyon Sop et al.* (Dist. D.C. November 18, 2022).
[228] "March 2023 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 7, 2023, at 48.
[229] Ibid., at 40.
[230] Ibid., at 49.
[231] "September 2022 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, September 7, 2022.
[232] "September 2023 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, September 12, 2023.
[233] Ibid.
[234] "March 2020 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 2, 2020, at 12-13.
[235] Ibid., at 47.
[236] Niharika Mandhana, James T. Areddy, and Michael R. Gordon, "*How Hong Kong Makes Evading North Korea Sanctions Easier*," *Wall Street Journal*, March 16, 2018.
[237] S.744, Ha Fa Trade International Co., Limited. Hong Kong Companies Registry, April 4, 2018.
[238] *S.746*, Ha Fa Trade International Co., Limited. Hong Kong Companies Registry, August 24, 2018.

[239] "March 2022 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 1, 2022, at 40-42.
[240] Hong Kong Companies Registry search data.
[241] *S.751, Cheng Xin Shipping Limited*. Hong Kong Companies Registry, October 7, 2022.
[242] 2021 Annual Return, Cheng Xin Shipping Limited. Hong Kong Companies Registry, September 26, 2021.
[243] Incorporation Form, Cheng Xin Shipping Limited. Hong Kong Companies Registry, September 13, 2016.
[244] 2021 Annual Return, Cheng Xin Shipping Limited. Hong Kong Companies Registry, September 26, 2021.
[245] Application for Deregistration of Private Company or Company Limited by Guarantee, Cheng Xin Shipping Limited. Hong Kong Companies Registry, May 16, 2021.
[246] Kang Kewen. Letter to the Board of Directors of Cheng Xin Shipping Limited. Grand Concept Certificated Public Accountants (Practising) Limited. Hong Kong Companies Registry, June 22, 2022.
[247] Notice of Resignation of Auditor, Cheng Xin Shipping Limited. Hong Kong Companies Registry, June 22, 2022.
[248] Incorporation Form, Cheng Xin Shipping Limited. Hong Kong Companies Registry, September 13, 2016.
[249] Singapore Titles Automated Registration System Report on Lot Number MK23-U11575L. Singapore Land Authority, last accessed June 11, 2024.
[250] *See, e.g.*, "North Korea: South seizes ship amid row over illegal oil transfer," BBC, December 29, 2017.
[251] Ibid.
[252] "March 2018 Report of the UNSC DPRK Panel of Experts," United Nations Security Council, March 5, 2018.
[253] "供油北韓 船隻港籍 船東廣州人," 華人今日報, December 30, 2017.
[254] Lawrence Chung, "Taiwanese man bailed over oil transfer to North Korean ship," *South China Morning Post*, January 4, 2018.
[255] Notice of Resignation of Company Secretary and Director, Win More Shipping Limited. Hong Kong Companies Registry, December 31, 2017.
[256] *S.744*, Win More Shipping Limited. Hong Kong Companies Registry, January 9, 2018.
[257] Notice of Appointment of Company Secretary, Win More Shipping Limited. Hong Kong Companies Registry, January 24, 2018.
[258] Striking Off Discontinued, Win More Shipping Limited. Hong Kong Companies Registry, January 30, 2018.
[259] Judgment, Win More Shipping Ltd. v. Director of Marine, *HCAL 1520/2018, H.K.S.A.R. High Court (May 2, 2019).*
[260] Ibid., para. 14.
[261] Ibid., para. 12.
[262] Ibid., para 18.
[263] Ibid., para. 19.
[264] Ibid., para. 20.
[265] Ibid.
[266] Ibid., para. 26.
[267] Ibid.
[268] *S.744*, Lighthouse Ship Management Limited. Hong Kong Companies Registry, August 28, 2020 (notice of striking off in three months); Notice of Resignation of Company Secretary and Director, Lighthouse Ship Management Limited. Hong Kong Companies Registry, May 29, 2018 (secretary resignation).
[269] 2024 Annual Return, Win More Shipping Limited. Hong Kong Companies Registry, January 26, 2024.
[270] Elizabeth Shim, "North Korea sanctions-violating ships to be released in the South," UPI, July 2, 2019.
[271] "Ling Yu: Oil/Chemical Tanker," Marine Traffic.
[272] Ibid.
[273] Ibid.
[274] Ibid, at 6.
[275] *See* "How to choose a charter type," Clarksons, last modified 2024.
[276] Chen's prosecution was not completed as he apparently committed suicide in June 2019. Elizabeth Shim, "Taiwan man jumps to death after North Korea sanctions violation," UPI, June 24, 2019.
[277] Associated Press and Agence France-Presse, "Taiwanese man sanctioned for oil sales from Hong Kong-registered tanker to North Korea," *South China Morning Post*, January 13, 2018.
[278] "Taking Additional Sweeping Measures Against Russia," U.S. Department of State, November 2, 2023; "Treasury Imposes Swift and Severe Costs on Russia for Putin's Purported Annexation of Regions of Ukraine," U.S. Department of the Treasury, September 30, 2022,; "Taking Additional Sweeping Measures Against Russia," U.S. Department of State, December 12, 2023; "U.S. Continues to Degrade Russia's Military-Industrial Base and Target Third-Country Support with Nearly 300 New Sanctions," U.S. Department of the Treasury, May 1, 2024; "United States Imposes Additional Sanctions and Export Controls on Russia in Coordination with International Partners," U.S. Department of State, May 19, 2023,; "Treasury Imposes Sanctions on More Than 150 Individuals and Entities Supplying Russia's Military-Industrial Base," U.S. Department of the Treasury, December 12, 2023.
[279] Echo Wong and Pak Yiu, "U.S. Treasury warned Hong Kong banks on tech exports to Russia," Nikkei Asia, July 6, 2023.
[280] Pak Yiu, "HSBC to halt corporate remittances to and from Russia," Nikkei Asia, last modified September 8, 2023.
[281] *"Executive Order 14114: Taking Additional Steps With Respect to the Russian Federation's Harmful Activities*," Executive Office of the President through National Archives, December 26, 2023.

[282] Pak Yiu and Echo Wong, "U.S. Treasury meets with banks in Hong Kong on Russia sanctions," Nikkei Asia, January 18, 2024.
[283] "Russia -related Designations; Publication of Russia-related Determination; Issuance of Russia-related General Licenses and Frequently Asked Questions," U.S. Department of the Treasury: Office of Foreign Assets Control, June 12, 2024.
[284] "As Russia Completes Transition to a Full War Economy, Treasury Takes Sweeping Aim at Foundational Financial Infrastructure and Access to Third Country Support," U.S. Department of the Treasury, June 12, 2024.
[285] "Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base," U.S. Department of the Treasury: Office of Foreign Assets Control, June 12, 2024.
[286] James Byrne et al., "*Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine*," RUSI, August 2022.
[287] "Sigma Technology Limited," Open Sanctions.
[288] *See Federal Express Corporation v. U.S. Dept. of Commerce*, No. 20-5337 (D.C. Cir. 2022) (rejecting a challenge to BIS power to issue fines on a strict liability basis); *Obligations of foreign-based persons to comply with U.S. sanctions and export control laws*, Department of Commerce, Department of the Treasury, and Department of Justice, March 6, 2024 (Joint Commerce, Treasury, DOJ note explaining that sanctions violations can lead to civil penalties under strict liability standard).
[289] Sheridan Prasso, "Chips From Texas Instruments and Other US Makers Flow Into Russia Despite Ban," Bloomberg, December 21, 2023.
[290] "Know Your Customer Guidance," U.S. Department of Commerce: Bureau of Industry and Security, last modified 2024.
[291] "A Framework for OFAC Compliance Commitments," U.S. Department of the Treasury, May 2, 2019.
[292] "Russian International Money Launderer Arrested for Illicitly Procuring Large Quantities of U.S.-Manufactured Dual-Use Military Grade Microelectronics for Russian Elites," U.S. Department of Justice: Office of Public Affairs, September 18, 2023.
[293] "*Executive Order 14114: Taking Additional Steps With Respect to the Russian Federation's Harmful Activities*," Executive Office of the President through National Archives, December 26, 2023.
[294] Secretary of State Antony Blinken warned Chinese officials during a visit in April 2024 that financial firm sanctions could be coming, and in June 2024 OFAC issued a guidance warning foreign financial firms to comply or face secondary sanctions. Takayuki Tanaka and Rintaro Tobita, "U.S. weighs sanctions on Chinese banks over Russia military support," Nikkei Asia, May 11, 2024; "Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base," U.S. Department of Treasury: Office of Foreign Assets Control, June 12, 2024.
[295] *Executive Order 13810: Imposing Additional Sanctions With Respect To North Korea*, The White House, September 21, 2017.
[296] *Executive Order 13902: Imposing Sanctions With Respect to Additional Sectors of Iran*, Presidential Documents, January 14, 2020.
[297] Special measures for jurisdictions, financial institutions, international transactions, or types of accounts of primary money laundering concern, *31 U.S. Code § 5318A*, Cornell Law School: Legal Information Institute.
[298] *For a summary of the statute and the powers it authorizes, see* "Looming Resurgence of FinCEN's Section 311 Authority," Clifford Chance, last modified March 2022.
[299] "Terrorism and Financial Intelligence 2024 Budget Request," U.S. Department of the Treasury, 2023.
[300] *Export Controls Enforcement Improvement Act*, S. 4085, 118th Cong. (2024).
[301] *See* Section IV.B.3 *above*.
[302] *See* "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," Financial Action Task Force, last modified November 2023, at 9 (Customer Due Diligence).

COMMITTEE FOR FREEDOM IN HONG KONG FOUNDATION

The Committee for Freedom in Hong Kong Foundation (**CFHK Foundation**) fights for Hong Kong and its people as China continues its crackdown on the city's freedoms. The CFHK Foundation defends political prisoners, free media, and Hong Kong people's right to live peacefully and freely after the handover to China in 1997. Hong Kong's fate is linked to the preservation of freedom, democracy, and international law in the region and around the world.

The Committee for Freedom in Hong Kong Foundation
1100 13th Street NW, Suite 800
Washington, DC 20005

For more information, please visit thecfhk.org.

COMMITTEE FOR FREEDOM IN HONG KONG FOUNDATION

The Committee for Freedom in Hong Kong Foundation (**CFHK Foundation**) fights for Hong Kong and its people as China continues its crackdown on the city's freedoms. The CFHK Foundation defends political prisoners, free media, and Hong Kong people's right to live peacefully and freely after the handover to China in 1997. Hong Kong's fate is linked to the preservation of freedom, democracy, and international law in the region and around the world.

The Committee for Freedom in Hong Kong Foundation
1100 13th Street NW, Suite 800
Washington, DC 20005

For more information, please visit thecfhk.org.