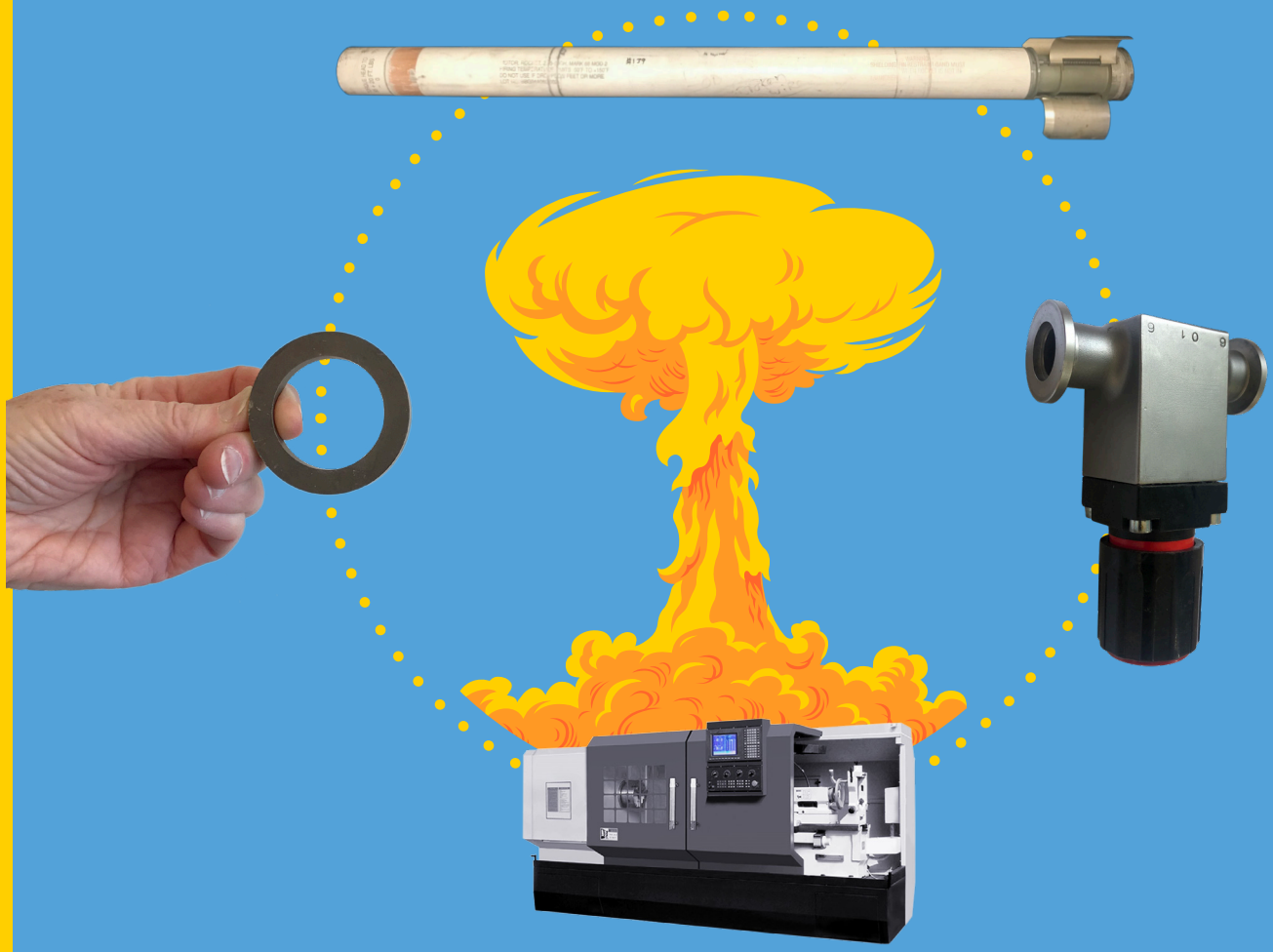
ILLICIT TRADE NETWORKS

VOL. 1

CONNECTING THE DOTS



BY DAVID ALBRIGHT, SARAH BURKHARD,
SPENCER FARAGASSO, LINDA KEENAN,
AND ANDREA STRICKER

Illicit Trade Networks

Connecting the Dots

Characterizing and Drawing Lessons
from Tactics and Methods of Illicit Procurement
to Improve Counterproliferation

Volume 1: Case Studies and Findings

By David Albright, Sarah Burkhard, Spencer Faragasso, Linda Keenan, and Andrea Stricker

Institute for Science and International Security

February 2020

This material is based on research sponsored by the United States Air Force Academy (USAFA) and Institute for Science and International Security under agreement number FA7000-18-1-0019. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

Distribution Statement A: Distribution unlimited of Volume 1 of Report

Cover design: Stewart A. Williams Design

Table of Contents

Volume 1

Volume 2 - Confidential: Iranian Networks: Drawing Upon the Cheng/Jamili Case Evidence

Executive Summary

Illicit procurement of strategic commodities is an ongoing threat perpetuated by states that operate outside of global nonproliferation norms and agreements. Such countries rely heavily on outside supply to obtain the commodities needed to build or augment covert or sanctioned nuclear, missile, and conventional military programs.

Many countries remain at risk for exploitation by state-directed illicit nuclear, missile, and military procurement networks, either by attempts to obtain sensitive and controlled equipment from their territories, or through the use of their territories in other ways, such as points for transshipment of those goods or as proliferation financing hubs. Driving the threat is also the fact that there has recently been an increase in the number of countries that make and supply strategic and dual-use goods in the developing world, creating greater availability of sensitive commodities worldwide. As adversaries seek to obtain the wherewithal to create and augment nuclear, missile, and military programs, the United States and its partners and allies must be better prepared to detect and stop those attempts. Despite many recent, particularly U.S.-led successes, stopping this trade remains difficult. Preventing illicit trade is imperative to U.S. and international security and to the creation of a world safer from the spread and use of nuclear and other destructive or destabilizing weapons.

In Volume 1, Section I, this report explains strategic commodity trafficking, or illicit procurement, to assist in understanding what this activity is, who is involved, and how it occurs. It explains the most basic activities of illicit trade and general structures of illicit networks. A series of illicit trade cases studies, focused on the ordering process, show key illicit procurement methods in action. Section II discusses the international framework of and recent developments in proliferation financing. It shows how illicit procurements are financed, with special emphases on cases involving Iran and North Korea. Section III explains how goods are shipped, once illicitly acquired, and also includes case studies. An annex to the shipping section discusses more on the main stakeholders involved.

Section IV, a special case section, draws out findings from a once-prominent transnational illicit network centered in China, the Cheng/Jamili network, which outfitted Iran's nuclear, missile, military, and other sensitive programs. David Albright, one of the authors of this report, was an expert witness for the United States Attorney for the District of Massachusetts on Cheng's 2016 sentencing hearing. Cheng pled guilty to six U.S. grand jury charges and was sentenced to nine years' incarceration. Albright was permitted to assess raw evidence in the case and much evidence was released publicly in the course of Cheng's trial. The detailed case information, including chat records, e-mails, and other associated documentation, is an enormously rich collection which also includes information about the activities of two other illicit trading networks. That which was open, or made public during the course of court filings, hearings, the trial, and sentencing hearing, is included in Section IV. This report contains a separate, confidential Volume 2 with additional content available to readers allowed under the rules of the court proceedings that was prepared with the permission of the U.S. prosecutor. Volume 2

is especially useful to U.S. counter-proliferation officials who have not had the opportunity to review this important enforcement case. Although Volume 2 is confidential, the lessons and insights from these cases are included in Volume 1.

The case studies in this report are focused on the ordering, financing, and shipping processes, and showcase key illicit procurement methods in action. Many of the case studies identify ways in which proliferant states and their associates seek and successfully obtain sensitive commodities. Other ones show when counter-proliferation methods have worked to thwart those efforts. These cases highlight ways in which countries can improve their detection and prevention of illicit procurement. The cases describe:

- types of goods sought, particularly those aimed at subverting, undercutting, or bypassing control lists on sensitive commodities;
- tactics for concealment;
- current and emerging methods of buying, shipping, and financing acquisition of controlled and sensitive commodities;
- nature of intermediaries working on behalf of proliferant states, and emerging trends and use of new kinds of intermediaries;
- methods of shipping goods from supplier to proliferant state, including routes and concealment methods; and
- methods of financing proliferation, including circuitous payment, money laundering, and virtual payment methods.

The cases identify intervention points for detecting and stopping illicit procurement including: points along the process of first contact with suppliers, ordering, checking of *bona fides* of customers, obtaining end-use and end-user certification for the sale of goods, export licensing, shipment arrangements, customs checks, and financing arrangements. The cases show where suppliers and governments can intervene or better detect illicit actors.

In Section V, the report ties together all the previous sections and makes available a large quantity of illicit procurement methods and tactics and their warning signs, commonly called "red flags." These methods and warning signs are drawn out of the cases and are of particular importance to governments and private sector actors. All parties must become aware of common and less common methods and warning signs of illicit procurement, and understand that better familiarization allows them to act as a net to detect and prevent illicit procurements from successfully making their way to proliferant states.

This section also recommends a range of policy steps that the United States and likeminded countries can take to more effectively detect and prevent illicit procurement today and in the future. The policy recommendations can help governments and private actors operationalize warning sign information and become more efficient at this goal.

Among the dozen recommendations are ways to improve the timely detection of illicit trade, expand outreach to the private sector, increase government/industry cooperation, better detect proliferation financing, and improve controls over shipping. The recommendations would also assist the enactment and tightening of sanctions against countries and their destabilizing weapons programs.

The policy chapter further recommends that the U.S. government more frequently exploit and comprehensively assess illicit trade evidence from federal or other prosecutions, on an unclassified, albeit confidential, basis. The information in these cases often points out new threats and loopholes to close, as well as methods for better thwarting illicit trade.

Countering proliferation financing remains a difficult area in which to make progress, but even as technology is exploited by illicit networks to route payments for goods, it can also be harnessed toward better detection of data that show illicit activity. Counter-proliferation financing efforts must continue to be bolstered internationally, requiring leadership by the United States, as the global financial center of the world economy. Defenses against cyber-hacking and electronic thefts of funds need to be improved as states increasingly turn to more virtual methods of funding proliferation.

Not enough has been done to prevent the misuse of shipping to obtain strategic goods. Transshipment of ill-gotten goods remains a major issue, and the use of front companies, freight forwarders, and free trade zones as intermediaries can create such complexity that it is nearly impossible to track the circuitous route of some illicit shipments to their final destination. Yet, customs, border, air, and maritime enforcement officials can better use intelligence and other data, combined with more sophisticated analysis, to conduct more sophisticated risk-based inspections. Moreover, despite the frequently unclear jurisdiction and complication of stopping goods in transit internationally, a complex web of international law supports and clarifies such interdictions on land, sea, and air.

The ultimate goal of U.S. and partner country policies should be to bolster their defenses and better hone their offenses in order to create a more functional counter-proliferation system as a whole. The findings and recommendations of this report aim to complement and strengthen U.S. government efforts in export licensing, outreach, intelligence, law enforcement, sanctions implementation, and other counter-proliferation programs, while anticipating and heading off future threats. It is our hope that this report contributes to efforts more broadly to prevent additional proliferation by adversaries of the United States and safeguard U.S. and international security.

Acknowledgements

This report is made possible in large part by support from the Project on Advanced Systems and Concepts for Countering Weapons of Mass Destruction (PASCC), U.S. Air Force Academy (USAFA). PASCC is supported by the Defense Threat Reduction Agency (DTRA). The material in this report is based on research sponsored by the USAFA and the Institute under agreement number FA7000-18-1-0019.

We thank an IT professional, who prefers to remain anonymous, for the long, *pro bono* hours spent on guiding us patiently through software to ingest and analyze emails and assess networks.

We are indebted to several technical experts who wish to remain anonymous. Finally, we thank the many law enforcement, counter-proliferation, and corporate officials who have worked for decades on efforts against strategic commodity trafficking and shared their experience and expertise with us.

It should also be noted that the opinions, findings, views, conclusions or recommendations contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the USAFA or the U.S. government.

Section I. Identifying and Ordering Strategic Commodities

Chapter 1. Introduction to Strategic Commodity Trafficking

Strategic commodity trafficking is the illicit trade in commodities, equipment, technologies, or material with direct or potential uses in nuclear, weapons of mass destruction (WMD), missile, or conventional military programs. It is central to outfitting numerous sanctioned, unsafeguarded, or otherwise dangerous military, ballistic missile, and nuclear programs. This trafficking largely stems from adversaries of the United States, including Iran and North Korea, and countries with tense relations with the United States, such as Pakistan and China. By violating U.S. and international laws and regimes, these countries engage in a criminal activity that arms them. For many developing countries, the acquisition of key goods will determine whether or not their sensitive weapons programs succeed.

Strategic commodity trafficking is defined as trade that is not authorized: 1) by the state in which it originates; 2) under international law; 3) by the state(s) through which commodities transit; or 4) by the state to which commodities are imported. One or multiple conditions in this definition can exist to qualify such trade as illicit, and therefore, prohibited.

Surreptitious acquisition of controlled goods helps a proliferant state develop or upgrade its advanced weapons capabilities. For developing countries, the pathway to acquiring advanced weapons and weapons systems typically involves the illicit procurement of strategic commodities from supplier nations. They illicitly seek outside supply of specific goods that they are unable to produce, or for which they lack specialized knowledge or manufacturing capabilities. The reasons include simply being unable to make reliable, highly-specialized goods essential for many military, ballistic missile, and nuclear efforts, or not having the funds to develop whole industries to make the goods – hundreds if not thousands of which are needed in these programs. Developed or newly industrialized countries are more independent from foreign supply but may also seek to illicitly upgrade or appropriate certain advanced technologies and equipment. They may face economic and technological hurdles to domestic production or want to acquire the goods from abroad, so as to copy them and learn to manufacture them on their own, often then relying on acquiring less sensitive subcomponents from abroad.

The interconnected and globalized marketplace facilitates the growth of illicit networks whose entities and operators live and work in multiple nations and territories and facilitate illegal transactions. These willing, *ad hoc* and regular intermediaries, as well as unintentional facilitators, fill orders on behalf of the so-called proliferant state and its illicit procurement organs. Illicit networks most often exploit licit business by attempting to secure sales by legitimate suppliers of controlled or sensitive goods. Operating from foreign locations can help conceal the nature of the sanctioned or sensitive state buyer through multiple countries, entities, and layers in a transaction. Through strategic commodity trafficking, states avoid the need for self-sufficiency in the means of producing advanced goods, and better achieve their military or strategic objectives.

Development of Strategic Trade Controls and their Uneven Implementation

Strategic trade controls were developed as a critical countermeasure against commodity trafficking in nuclear, missile, WMD, and military-related goods. Although no one tool can completely stop determined countries like Iran and North Korea from acquiring illicitly the goods they seek, strategic trade controls, especially when teamed with sanctions, have proved important in slowing and complicating those efforts. They have also stimulated the development of and provided tools to responsible nations for better and earlier detection of illicit efforts to create advanced weapons systems, particularly in regions of tension or conflict, such as North and Central Africa, the Middle East, South Asia, Northeast Asia, and Central America. By detecting illicit procurement efforts earlier and causing delays, strategic trade control systems have provided more time for diplomacy and other tools to succeed at finding non-military solutions. A principled goal of strategic controls is to allow greater opportunities to achieve peaceful outcomes in regions of tension, instead of arms build-ups and arms races that can lead to destabilization and conflict.

In the endeavor to thwart commodity trafficking and bolster strategic trade controls, the passage of United Nations Security Council resolution (UNSCR) 1540 in 2004 was an important milestone. It recognized the need for all nations to put in place appropriate, effective trade controls to prevent the spread of the wherewithal to make weapons of mass destruction. Yet, the resolution today remains under-implemented and levels of state compliance are irregularly reported. UNSCR 2325, passed in late 2016, lays out many steps and actions for addressing these shortcomings. It also highlights the need for more attention to enforcement, counter-proliferation financing measures, and transshipment controls.

Today, strategic trade control laws are well implemented in supplier countries. For example, the Nuclear Suppliers Group (NSG) has established a wide range of norms and principles over several decades for its members, as well as extensive control lists of equipment, materials, and technology relevant to nuclear proliferation. However, cases of nuclear commodity trafficking show that some NSG countries implement and enforce their laws far better than other members. Moreover, about three quarters of all countries and territories are not members of the NSG. These non-NSG states often have far weaker strategic trade control laws, or none at all.

Strategic trade control systems by their nature are complicated and have often been developed *ad hoc*. It is a challenge to assess their strength in individual countries and draw findings about how well they work nationally and globally. A separate Institute analysis, the *Peddling Peril Index (PPI),* ranks the strategic trade control systems of 200 countries, territories, and entities, according to their strength and performance and makes targeted recommendations to improve those systems based on the particular level of economic development of countries.[1] It found in

[1] David Albright, Sarah Burkhard, and Andrea Stricker, *The Peddling Peril Index for 2019/2020, Institute for Science and International Security,* May 23, 2019, http://isis-online.org/uploads/isis-reports/documents/ThePeddlingPerilIndex2019_POD.pdf

its 2019/2020 update a wide variation in the effectiveness of national strategic trade controls and sanctions, assessing that even the most advanced nations face challenges and can improve their controls.

Countries could receive a total of 1,300 points in the PPI. Figure 1.1 shows that scores ranged between about -200 and 1,000 points, meaning that no country received more than 80 percent of the possible points, and a few countries received negative scores. The point ranking for the 200 countries was fundamentally bimodal. One peak illustrates that about a quarter of countries maintain fairly robust, albeit not perfect, national strategic trade controls, such as comprehensive legislation and effective implementation, and the other peak shows that about three quarters of countries have far less effective systems. The PPI found that some 120 countries do not have export controls in any general sense.

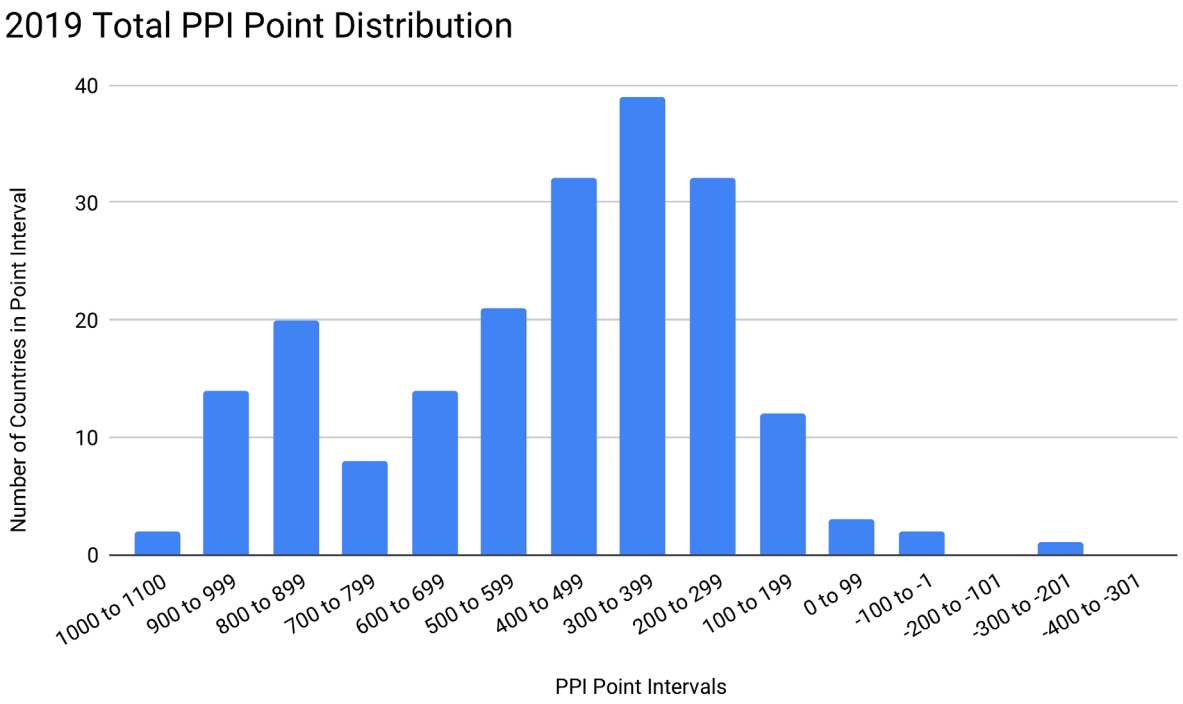


Figure 1.1. Distribution of total points received by 200 countries in the *Peddling Peril Index for 2019/2020*, in intervals of 100 points.

The PPI found that only a fraction of the world's national trade control systems received more than 50 percent of the available points under the index. Twenty-nine countries achieved two-thirds or more of the available points, and an additional 21 countries achieved more than half but less than two-thirds of the possible points. However, the remaining 150 of the 200 evaluated countries received less than half of the available points. Ninety-six countries received less than one-third of the total points. Given the unstoppable pace of globalization and the central importance of strategic trade controls in stopping proliferation, this wide range of performance is alarming.

Figure 1.2 is a pictorial representation of the 2019/2020 *Peddling Peril Index's* scores for each country, territory, or entity. Dark blue represents higher scores and light blue represents lower scores. In general, the scores in the northern hemisphere were higher than in the southern hemisphere, and developed nations scored higher than developing countries.

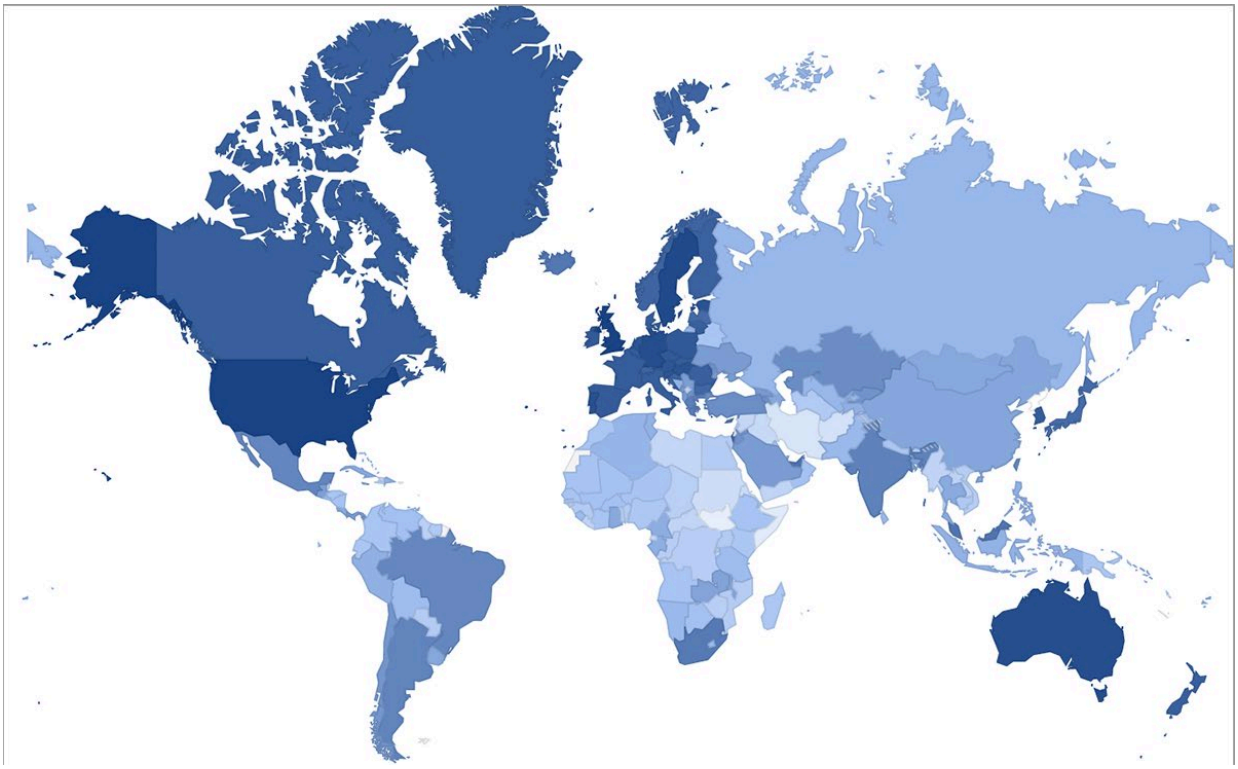


Figure 1.2. The PPI scores represented by country, where darker blue indicates a higher score.

Policymakers are attempting to combat the problem of illicit procurement that is exacerbated by a lack of export controls in over half of the countries and territories evaluated. This underscores the importance of understanding the tactics and methods used by illicit procurement networks so that states can best detect and prevent attempts as they occur, as well as identify future methods that networks will likely use against them.

Evaluating weaknesses in national trade controls before instances of illicit procurement occur involves assessing where, how, and at what point in the supply chain failures are most likely to take place. This allows opportunities to design policies ahead of time that will prevent failures, and ideally, prevent the emergence of additional proliferant states and augmented weapons programs. Understanding these weaknesses can allow for predictions about where undiscovered tactics are being used and preventative measures that can be taken before likely, future schemes occur.

Dynamic Nature of Illicit Trade

Trade control systems face ongoing challenges in that states and their illicit procurement networks are constantly evolving and attempting to evade controls. A newer challenge is that illicit networks or proliferant states set up their own supply chains to manufacture goods, since their challenge at the core is that they cannot rely on domestic supply or know-how. A pioneer in this approach was the A.Q. Khan nuclear proliferation network, run out of Pakistan's sanctioned nuclear weapons program. It started in the 1970s with a goal of building a gas centrifuge enrichment facility in a country with limited manufacturing capabilities. It grew until it peaked in the 1990s and early 2000s, having successfully built centrifuge plants in Pakistan to make weapon-grade uranium for nuclear weapons and supplied gas centrifuges to Iran, Libya, and North Korea. This network established an extensive, off-shore, transnational manufacturing network, with capabilities such as manufacturing many gas centrifuge components for uranium enrichment in Malaysia, training in the United Arab Emirates, and other network nodes in Switzerland and South Africa that could make essential equipment for a centrifuge plant.[2] However, this network also had to depend on pre-existing suppliers for not only the most sensitive goods, but also less controlled or non-controlled goods.

Another challenge is that although many suppliers of strategic goods exist today in states where trade controls are well-implemented, with increased globalization, more of these suppliers have emerged elsewhere or have established distributors in countries where trade controls are poorly implemented. Moreover, as the means of manufacture spread to developing countries without trade controls, the risk grows that such technologies will lead to the easier transfer of controlled or sensitive goods to proliferant states and their networks. All illicit networks exploit transshipment hubs, or countries where fewer restrictions are in place over the movement and transit of goods. Free Trade Zones (FTZs) are one example of such territories. Illicit networks can claim a transshipment point is the end destination of a consignment simply by establishing false or front companies and misstating the end use of the goods. They also use multiple layers of financial transaction routes to pay for goods, thereby obscuring to target state authorities and responsible financial institutions where money originated and what it is intended for.

In a general sense, whatever their specific *modus operandi,* illicit networks or agents are not, for example, drug traffickers, and must penetrate and integrate themselves into a world of existing suppliers and trading companies, which are tricked into selling goods inadvertently, are willing to turn a blind eye to the nature of the potential customer, or are willing conspirators in an illegal effort. Corrupt insiders in supplier companies can pose particular challenges. When all these actors cooperate, knowingly or unknowingly, and using the most practiced and tested methods, they can thwart strategic trade control systems and be exceedingly difficult to stop. Evading countermeasures on the part of adversaries often means that counter-proliferation is a continuous effort that requires new and more targeted efforts to close gaps. Too often, it is the

[2] David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010).

adversary that stays ahead of the game. This dynamism is to be expected, but it should be better anticipated and countered.

It is vital to recognize the tactics and methods of illicit procurement networks before they can successfully procure the goods they seek. It is also imperative to stay ahead of their evolving methods and prepare for and anticipate future threats. On a tactical level, countering strategic commodity trafficking relies most fundamentally on understanding how the adversary operates.

Structure of Illicit Procurement Networks

An illicit procurement network is made up of multiple entities and individuals. They aim to procure nuclear direct, WMD, missile, and military-use goods as well as dual-use goods, or those with both military and civilian applications. Many target commodities are controlled by national and international trade control regimes and laws. The organization of these efforts has a network structure, which differs, for example, from a hierarchical structure. A hierarchical structure entails all entities subordinate to a primary entity. A network in the strategic commodity trafficking sense is made up of an interacting collection of entities and individuals engaged in the process of procuring strategic commodities, with no clear hierarchical structure. A network structure includes all aspects of the activities necessary to organize the acquisition of goods and deceive suppliers, including ordering goods, paying for them, and shipping them.

A network is a collection of "nodes" which can represent a company or entity, an individual, a state-owned or operated procurement organization, or a state nuclear, WMD, missile, or military program. These nodes are connected by interactions, typically represented by lines, which can represent initial "inquiries" for a price quotation about commodities, orders, shipments, and payments. A node that has many connections is referred to as a hub. A hub could be the sensitive program itself, a domestic procurement organization operating on its behalf, or a particularly active trading company located outside the proliferant state that seeks many goods from a variety of suppliers. Other hubs can include shipping hubs, transit hubs, and proliferation financing hubs. Each should be understood to be a center of major activities where some loose direction or coordination occurs to ensure all the network's nodes are effective, whether aware or unaware of the nature of the network's activities—including companies, shipping agencies, middlemen or brokers, and banks. In other words, they must be securing the needed goods for the proliferant state's sensitive or sanctioned programs. Illicit procurement networks must at some point abuse normal trade arrangements to obtain these goods.

Illicit procurement networks are usually comprised of at least several of these major components—each a proliferation node, or hub, if the node is particularly active. Many networks have some or all the following main components, such as:

- A state nuclear, WMD, missile, or military program or complex which compiles lists of needed goods;

- A domestic procurement organization which receives the lists of needed equipment from the state program and organizes their procurement domestically and abroad;
- Domestic front or trading companies that often work under contract for the procurement organization to obtain goods;
- Other front or trading companies or middlemen/brokers, usually located abroad, and further removed from the proliferant state's procurement organization. They are recruited or hired by the procurement organization or its domestic procurement companies for the purpose of placing orders for goods and also potentially receiving them in another country;
- Legitimate suppliers of goods;
- Subsidiaries of legitimate suppliers of goods;
- Intermediaries involved in shipping and logistics;
- Banks, financial institutions, or informal payment structures which wittingly or unwittingly facilitate financing for goods.

Networks of traffickers, suppliers, and trading companies are connected by requests for price quotes on goods, orders, shipments, payments, and other communications and transactions. In network parlance, these connections are represented by lines connecting the nodes.

There are a variety of individuals who are part of an illicit procurement network. Typically, procurement experts working within the state program or complex and its procurement organizations are at the center or comprise a core hub of the network. Business, financial, and logistical people are in outer nodes surrounding the hub. They are more removed from the state complex and are closer to the supplier. Figure 1.3 shows an illicit procurement network with the key procurement actors located at the center. The entities and actors that comprise the core of the network are often removed from contact with the supplier, making them difficult to detect behind any procurement attempt.

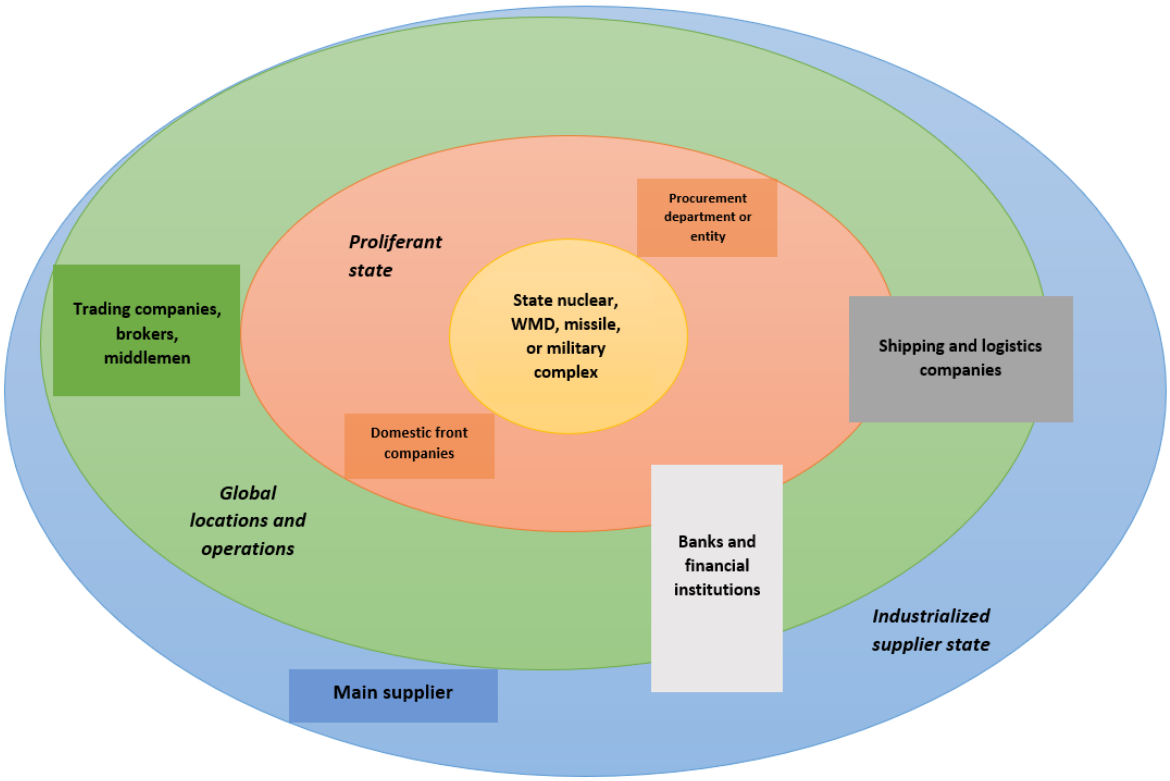


Figure 1.3. Depiction of actors and entities in an illicit procurement network. (No connecting lines are included for the sake of clarity).

A domestic trading company that contracts with the state's procurement organization may be engaged in a range of legitimate business activities in addition to illegal ones. It may seek goods from abroad directly from suppliers or indirectly via other trading companies located in other countries. Sometimes, these trading companies or agents will even find a legitimate manufacturer in a third country to order the goods from a supplier.

The covert state weapons program or its procurement organization may directly establish its own front companies, either domestically or off-shore, or contract with local trading companies to acquire goods from abroad. Domestic trading companies and certain foreign ones, in general, know that their purchases for the state are illegal. Moreover, a front company may be little more than a postal address, and trading companies can easily change their name. The company's name may have multiple operators associated with it, as a means to hide its existence from authorities and its connection to the state program.

Front and trading companies play an important role in the ordering process. Their goal is to find a supplier of the goods, despite trade controls and suppliers' internal compliance systems aimed at defeating illicit procurement. To achieve that goal, they research suppliers via the internet, trade shows, or their own contacts, and contact the supplier, often initially via an e-mail seeking a price quotation for specific goods, where they are trying to appear like a legitimate customer. At the same time, they may contact a number of other suppliers, and also

subsidiaries of the same company, or additional sales managers, probing for a "weak link" that is willing to provide the goods. Once the front or trading company finds a willing supplier, it needs to place an order and arrange for delivery and payment.

An illicit procurement network may also seek the services of a broker to obtain goods or other services. Trade control laws traditionally have been slow to control the brokering of purchases of dual-use military and civilian goods, unless their use in a weapons program is demonstrated. An intermediary or broker may be located in one country and arrange the purchase of goods from a different country and their transport to still another country, or even the country hosting the covert weapons program. In addition, a broker may assist in providing insurance, financing, and transportation and logistics. Brokers are often individuals operating small companies and are usually mobile and able to operate from many states.

Basic Activities of Illicit Procurement Networks

There are three basic activities of illicit procurement networks. They seek to: 1) order and purchase a controlled or sensitive commodity, 2) finance the purchase of the commodity, and 3) ship the commodity. Each of these activities is often conducted with the intention of obscuring to the supplier and its government (unless either are complicit) that the actual end-user and end destination of the commodity is a state that is not authorized to import it. The latter could also include non-state actors.

Figure 1.4, showing a Pakistani military equipment trafficking network, illustrates a network carrying out all the facets of an illicit procurement scheme—ordering, shipping, and payment. It shows many of the components described above. As stated, not all such networks will contain each of the components listed.

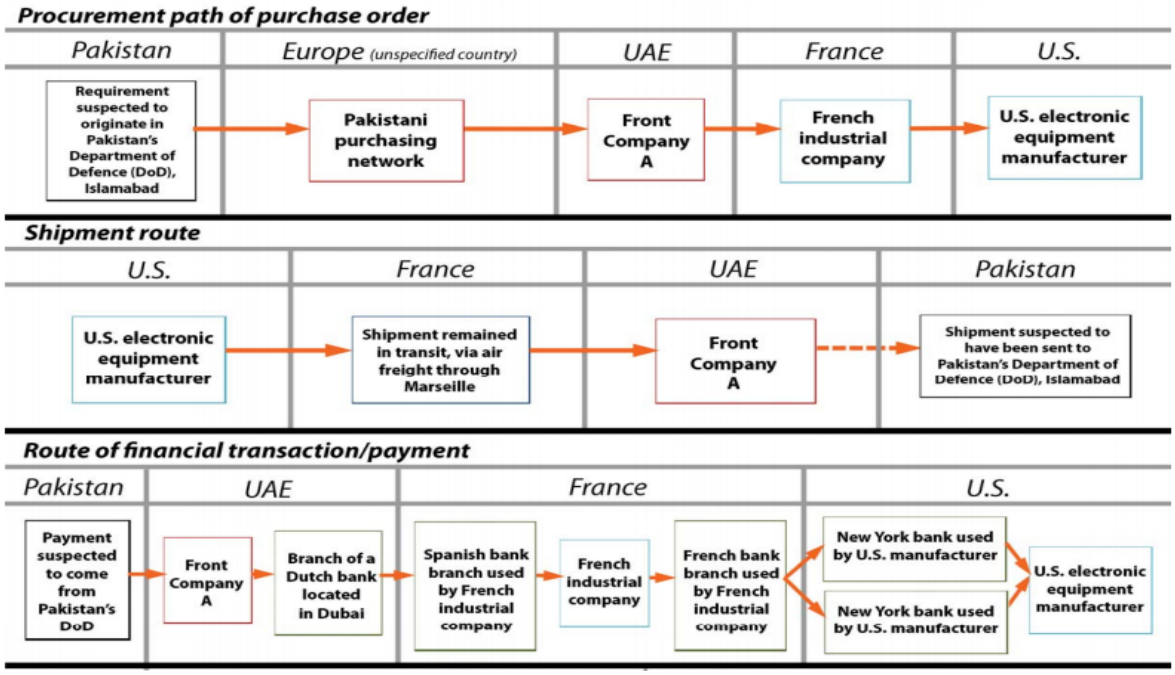


Figure 1.4. Pathway examples of an illicit procurement network's activities.[3] This figure shows the flow of orders, shipments, and financing through a network. (UAE stands for United Arab Emirates).

Globalization and the ease of international travel, communication, and trade has provided illicit procurement networks with many opportunities to obtain goods for covert or sanctioned weapons programs. These networks try to mask their procurements as legitimate trade. The purpose of the various intermediaries is to help hide the identity of the actual end-user from the supplier and authorities. Sometimes intermediaries in a network are unaware of the actual end use of procurements, but other times they are aware or choose to turn a blind eye to the true purpose of the goods. A more frequently observed tactic today is an illicit procurement agent establishing a trading company located in the supplier state. That way, they avoid the need for suppliers to concern themselves with exports or licensing. Once they obtain the goods, they can furtively arrange illicit shipping themselves. Since the illicit agent is the individual preparing shipping documentation, they can easily falsify the description of contents, which evades the vigilance of customs controls and shipper due diligence efforts. A more elaborate scheme involves the creation of an off-shore supply chain that both procures and produces needed dual-use goods and delivers them to the end-user. Figure 1.5 summarizes an increasingly complicated set of schemes to acquire goods illicitly.

[3] Figure from case study by David Albright, Paul Brannan, and Andrea Scheel (Stricker), "Pakistan's Illicit Procurement of Missile and Drone Equipment Using Multiple Financial Transactions," *Institute for Science and International Security,* January 28, 2009, http://isis-online.org/uploads/isis-reports/documents/Pakistan_Financial_28January2009.pdf

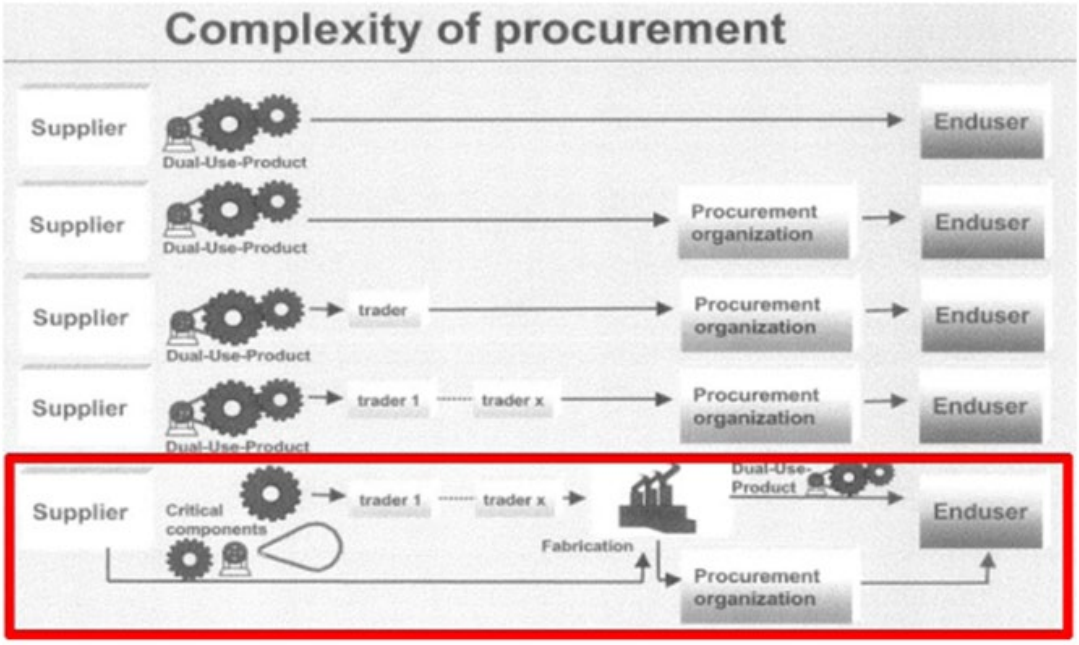


Figure 1.5. Schemes to obtain sensitive goods and overcome strategic trade controls and sanctions, listed from top to bottom by increasing complexity. The red outline around the last scheme is in the original source and emphasizes the more elaborate scheme of manufacturing critical components off-shore and fabricating them into a finished good, in addition to sending dual-use goods to the end-user. Source: Financial Action Task Force, *Typologies Report on Proliferation Financing*, June 18, 2008, https://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

Illicit procurement networks place orders for goods in or from countries with weak trade controls that experience high volumes of international trade, frequently using Free Trade Zones to hide illegal re-transfers of goods to the ultimate end-user, the proliferant state. To obtain goods in supplier countries with well-developed export controls, the networks rely more on false end-user statements and fraudulent shipping documents. Shipments and payments are arranged with the intention of hiding the true end-user.

For many of the types of goods sought by an illicit procurement network, such as dual-use goods, the network members must falsify an end-use statement, a critical document required by most exporting countries in the process of granting licenses. A network will try to establish for the supplier that the end use is in a country that is not subject to sanctions or controls on certain goods. It will try to show that the end-user is a company or entity that has a legitimate need for the goods. Or, the agents will claim the end-user is in a country that has weak or non-existent export controls, so when the goods are sent to this third country, they can be more easily re-transferred to the state that is banned from receiving them.

The international shipment of illicitly-obtained goods often involves large transportation centers where cargo is sorted and redistributed for shipment onward. Previously, major illicit

shipping nodes have included the United Arab Emirates (UAE), Hong Kong, Singapore, and Malaysia. Both freight forwarders and Free Trade Zones, or other special economic zones, are sometimes used as the declared end destination of goods actually destined for another country. Often, these zones have less stringent export controls than the rest of the state, making it easier for the illicit procurement network to re-transfer goods to their final destination.

Paying for illicitly acquired goods requires access to the international financial system, and the source of the funds for those goods must be hidden from law-abiding financial institutions and national authorities. Rarely does a proliferator use bags of cash. Purchases are made from legitimate suppliers which expect to conduct business, including being paid, in a normal, legitimate manner. Trading companies and intermediaries also expect a profit for their efforts.

Schemes to route money from the actual end-user to the supplier and intermediaries can be complex, involving more than one bank and multiple transfers across borders. It is difficult for financial institutions to detect the illicit nature of transactions, even though they often employ extensive compliance departments and personnel, as well as advanced software designed to detect money laundering and other illicit finance that would run afoul of domestic financial laws and sanctions. If required, any description of the reason for a payment can be falsified. Transactions can also be split in order to fall below reportable transaction thresholds in many supplier states.

Moreover, illicit procurement networks carry out multiple cross-border transactions to conceal the origin of a transfer, for example, from a sanctioned country's bank to a second country's bank that does not levy sanctions against it, and then from that bank to the bank account of the supplier in its country. Additional transfers can occur in-between to further obscure the original source. The development of proliferation financing controls is in its infancy, making the financing of proliferation one of the more difficult to detect activities conducted by illicit procurement networks, unless they are new to illicit activity and leave behind obvious signatures.

Chapter 2. Case Studies: Orders, Inquiries, and Flow of Goods

A set of case studies is presented in this chapter to show how illicit procurement networks function and operate, and in particular, how they make initial inquiries about purchasing products and then submit orders. They also show how the goods successfully make it to the proliferant state.

Case 2.1: Vast Iranian Illicit Military Procurement Network shifts operations to different countries once uncovered[1]

On September 17, 2008, the U.S. District Court of the Southern District of Florida unsealed a federal grand jury indictment against sixteen foreign individuals and companies involved in procuring items with military applications for Iranian entities through Dubai and Malaysia-based illicit procurement networks. Those under indictment allegedly circumvented U.S. export controls by utilizing a transnational network of firms located throughout the world to successfully purchase and channel the controlled goods to Iran. The dual-use goods obtained by the network included electronic components capable of being used to construct Improvised Explosive Devices, or IEDs, such as field-programmable gate arrays, integrated circuits, Global Positioning Systems (GPS), Field Communicators, and microcontrollers. The same types of items have been found in IEDs used against U.S. troops in Iraq and Afghanistan.

In March 2005, the United States reportedly learned of the Mayrow General Trading Company's activities, which were primarily rooted in the UAE, and to a lesser extent, in Malaysia, and started pressuring the UAE government to stop this company. The UAE resisted U.S. efforts. Finally, in March 2007, the UAE government shut down Mayrow General Trading Company. Mayrow was no longer involved in a Malaysia-based network after February 2007. An entity called Vast Solution had an increased role in the network after Mayrow was closed. The Malaysia network, centered at Vast Solution, appears to have gradually replaced the Dubai network entirely.

The Commerce Department's Bureau of Industry and Security added one hundred and eight individuals associated with the network to the Entity List on September 22, 2008. U.S. companies are barred from engaging in business with them. In 2006, the Commerce Department had placed sanctions on the core set of 16 entities and individuals mentioned in the indictment. To date, none of the entities and individuals involved in the case are known to have been prosecuted or extradited to the United States to face charges.

Dubai Network: The individuals allegedly responsible for operation of the Dubai-based network are accused of lying on U.S. end-user declaration documents for items, which allegedly went to entities in Iran in violation of the U.S. embargo. Two chief executives of the

[1] United States District Court of the Southern District of Florida, *Superseding Indictment: United States vs. Ali Akbar Yahya, F.N. Yaghmaei, Mayrow General Trading et al.*, September 11, 2008.

import/export company, Mayrow General Trading Company, allegedly utilized this company as the anchor of the Dubai and Malaysia-based illicit trade networks. These individuals, one indicated in the indictment to be of Iranian birth, allegedly held managerial or associate roles at other UAE-based companies in the network. These companies included Atlinx Electronics, Micatic General Trading, and Majidco Micro Electronics. Iranian companies named in the U.S. indictment that received items include Toos Electronics and Neda Industrial Group. Neda Industrial Group had offices in Dubai and Tehran. Additional companies or entities located in Iran may have been part of the Mayrow scheme, but they are not specified by name in the U.S. indictment. Under the Dubai operation, 18 alleged cases of illicit trade occurred or were attempted (see Figure 2.1). In some cases, the U.S. indictment is unclear about whether items successfully reached Iran.

The trading companies effectively created a wall between the Iranian entities and the U.S. suppliers, making it difficult for the U.S. suppliers to identify the true end-user of an item (Figure 2.1). In Dubai, these four companies, all with the same address and managed by the same two managers, placed most of the orders. This strategy of dividing up the orders reduced the "signature" of each trading company to prying authorities and potential suppliers, increasing their chance of success.

The shipment routes of the ordered items were also designed to hide the true end-user. Allegedly, the two primary individuals responsible for operating the Dubai network often sent purchase orders to U.S. companies requesting electronic items for Majidco, Micatic, and Mayrow, and then facilitated payment for the items through Mayrow and other companies. The two individuals and their associates allegedly colluded to obscure the identity of the final end-user from U.S. export authorities by falsifying export documents. According to the U.S. indictment, once the items were exported to the UAE entities, they were then diverted or re-exported to the Neda Industrial Group in Tehran or to other Iranian companies.

Example illicit procurements: In January 2004, Majidco Micro Electronics allegedly placed an order for 7,500 Microchip brand microcontrollers through the Amsterdam, Netherlands subsidiary of a Chandler, Arizona company. Upon receipt of the items, Majidco allegedly diverted or re-exported them to the Neda Industrial Group. This same Arizona company's Dublin-based subsidiary was likely targeted for an additional 5,000 microcontrollers in July 2004, which were also sent to Neda Industrial Group.

Another case, occurring also in January 2004, allegedly involved an unnamed individual who brokered for Atlinx the export of 120 field-programmable gate arrays from a Mountain View, California company using a phony end-user statement that claimed the shipment would ultimately go to Heliopolis, Egypt. In February, the items were allegedly exported to Atlinx Electronics, and in March, they were received by an unspecified company located in Iran.

According to the indictment, in May 2006, Mayrow General Trading also arranged for the export of Invensys Model 375 Field Communicators from a Foxboro, Massachusetts company to

a company called Telectron, located in Abu Dhabi, UAE. Later that month, an unnamed entity in Iran allegedly received these items.

Twelve similar procurements relying on phony end-user declarations led to a total of eighteen alleged instances of successful or attempted illicit trade by Mayrow and its UAE-based affiliates through the end of 2006 (Figure 2.1). Iran appears to have used trading companies to develop successful procurement paths, and then abandoned or modified those paths when they were no longer successful or were in danger of being exposed.

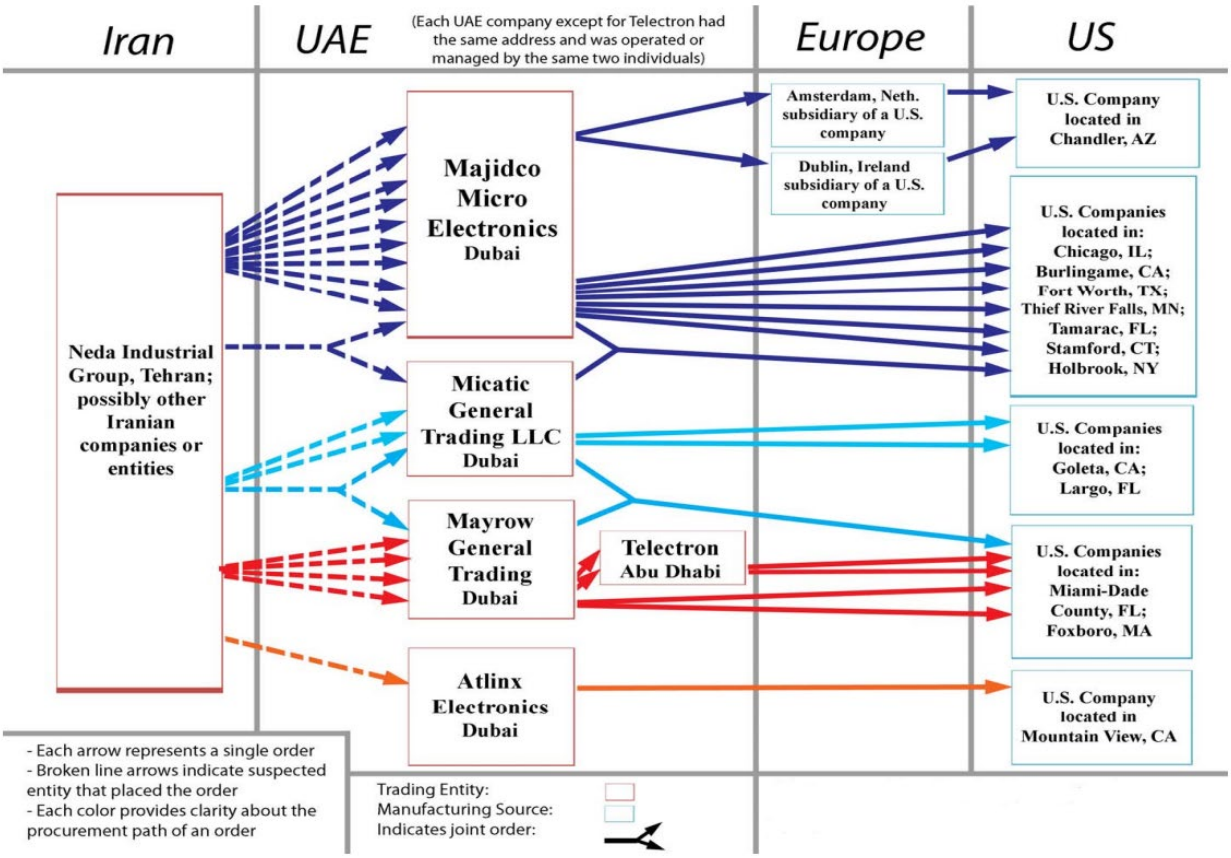


Figure 2.1. Order routes used by the Dubai network in the scheme.

Malaysia Network: Beginning in at least October 2006, Mayrow General Trading Company in Dubai and its affiliates based in Malaysia allegedly began to procure items from U.S. companies. These items were allegedly exported from the United States to British, German, and Singaporean companies before being diverted or re-exported to Iran in violation of the U.S. embargo against Iran. A company in Malaysia called Vast Solution was allegedly the anchor of the Malaysia-based network, and its associates had ties to Mayrow and other UAE companies, according to the indictment. Vast Solution was allegedly operated by an Iranian citizen living in Malaysia. Under the Malaysia operation, 13 alleged cases of illicit trade occurred or were attempted. Figure 2.2 shows the scheme pictorially.

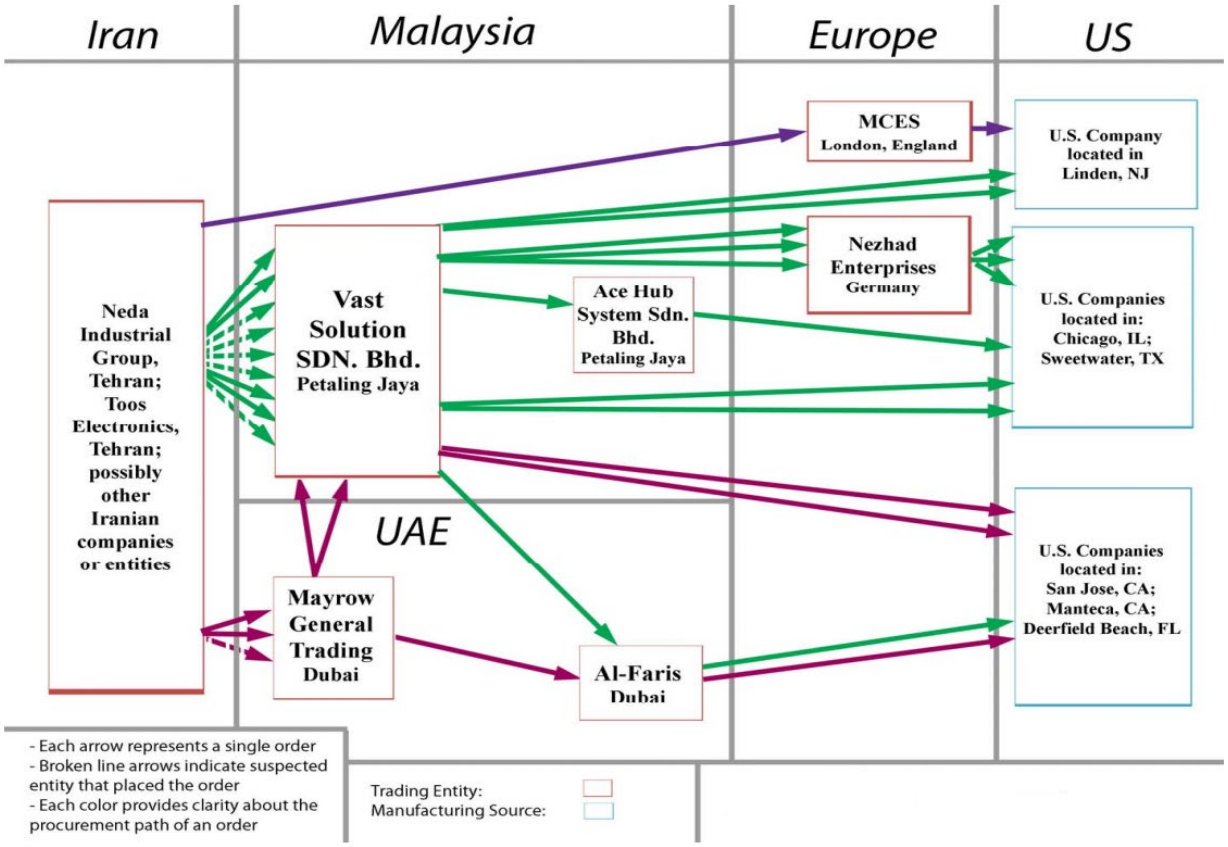


Figure 2.2. Order routes used by the Malaysia network in the scheme.

This case study, based on allegations contained in the U.S. indictment, illustrates the major problem posed by countries of diversion concern, or states whose companies or entities receive goods that are diverted or re-exported and ultimately utilized by proliferant states. The UAE's port capital of Dubai, for example, functions as one of the world's most unrestrictive free trade and shipping zones. While Dubai has taken steps in recent years to improve its export control implementation, it continues to be exploited by front companies that actively procure dual-use items for entities in countries under sanction.

This case study also demonstrates that the strict export control system of the United States remains susceptible to exploitation by transshipment schemes. It is difficult for manufacturers and suppliers to know when they are being exploited by sophisticated illicit procurement networks. The successes of the Dubai and Malaysia-based networks in obtaining the items show that U.S. companies are often unable to detect illicit procurement schemes on their own and require the help of governments to inform them about current schemes targeting their products, suspicious entities and purported end destinations of products being used by illicit procurement networks, and even help assisting them in making a determination about selling goods when they have concerns.

Case 2.2: Pakistani Illicit Nuclear Procurement Network attempts the "barrage approach"[2]

In late 2006, the export control office at a large European vacuum manufacturer noticed a suspicious pattern of inquiries from trading companies in Pakistan and Dubai for vacuum pumps and repair kits. The manufacturer's export control office suspected that the items were for use in Pakistan's gas centrifuge uranium enrichment program and ignored the inquiries. This office adheres to the company's internal compliance program and receives and analyzes suspicious inquiries from the manufacturer's many subsidiaries and sales agents. It functions as a hub of a network aimed at detecting and stopping potential illicit procurement attempts. In short, it functions as a "detection hub."

Pakistan's uranium enrichment program needs to regularly repair and replace broken centrifuge equipment, including vacuum equipment that is vital to the operation of gas centrifuges. Pakistani government procurement agents enlist trading companies to probe the global market in efforts to buy these goods illicitly. Throughout 2007 and 2008, the Dubai and Pakistani trading companies in this case study continued to seek items suspected to be for Pakistan's unsafeguarded nuclear program.

The global market in dual-use goods is enormous; the market in vacuum items is an important subset of this international market. Almost all of this business in dual-use items is legitimate. Illicit procurement inquiries from smuggling networks are estimated to make up less than a tenth of one percent of the total number of inquiries received by this supplier. The small fraction of suspicious inquiries makes detecting these inquiries challenging. To overcome this obstacle, the manufacturer has empowered its export control office to review inquiries and train company personnel to spot suspicious procurement patterns. The company's export control office then relays advice based on its analysis to its sales agents.

This case shows that trading companies engaged in illicit procurement are aware that their inquiries will often be met with skepticism and that many will be ignored and unfulfilled. As a result, the trading companies might send out inquiries for the same items to as many manufacturers and their foreign sales agents as possible. The illicit trading companies also try to exploit any lack of communication among a single manufacturer's sales agents by sending a barrage of inquiries to many of its sales agents within a short period of time, or all at once. Without a centralized export control office, the individual sales offices of a manufacturer would be unaware of the identical inquiries sent by the same trading company to other sales offices.

Further complicating the situation for the manufacturer, the items listed in the inquiries are often not explicitly controlled; therefore, simply examining the items requested does not reveal the illicit procurement attempt. In this case, instead of looking only at the items in the inquiry, this manufacturer's export control office focused on the specific trading companies and

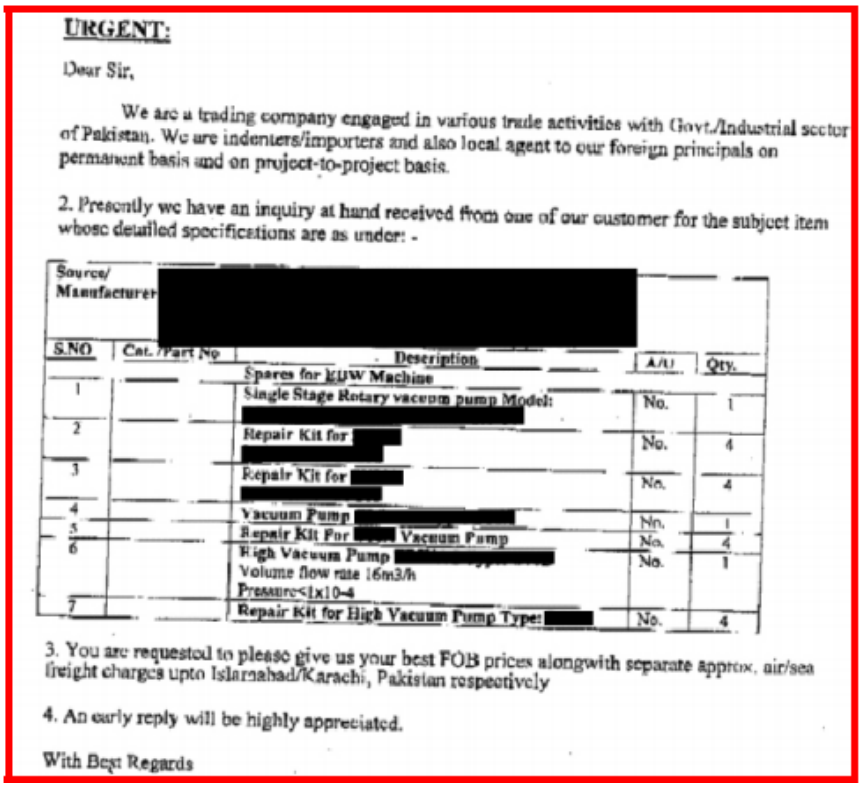
[2] Case information provided by an anonymous European vacuum equipment manufacturer.

declared end-users or lack thereof, from where the trading companies were sending their requests, and how often they repeated these inquiries to other sales offices.

Example of illicit procurement attempts: On October 14, 2006, Trading Company A, a suspected Pakistani procurement agent for the country's sanctioned nuclear program, sent identical inquiries for vacuum pumps and repair kits to four of the manufacturer's sales agents in Germany, the Netherlands, and France. Five days later, Trading Company A sent the same inquiry to another European sales agent for the manufacturer.

Also on October 14, 2006, Trading Company A sent a separate inquiry for a different set of vacuum pumps and repair kits to the manufacturer's office in Germany. Two days later, another trading company (Trading Company B) based in Dubai, sent this same inquiry to the manufacturer's sales office in Germany and another in Singapore. A little over two weeks later, Trading Company A yet again sent this same inquiry to the manufacturer's sales office in Germany.

Figures 2.3 and 2.5 show copies of the initial inquiries submitted by the network, and Figures 2.4 and 2.6 indicate the scheme pictorially.



URGENT:

Dear Sir,

We are a trading company engaged in various trade activities with Govt./Industrial sector of Pakistan. We are indenters/importers and also local agent to our foreign principals on permanent basis and on project-to-project basis.

2. Presently we have an inquiry at hand received from one of our customer for the subject item whose detailed specifications are as under: -

Source/ Manufacturer: [redacted]

S.NO	Cat. /Part No	Description	A/U	Qty.
		Spares for KUW Machine		
1		Single Stage Rotary vacuum pump Model: [redacted]	No.	1
2		Repair Kit for [redacted]	No.	4
3		Repair Kit for [redacted]	No.	4
4		Vacuum Pump [redacted]	No.	1
5		Repair Kit For [redacted] Vacuum Pump	No.	4
6		High Vacuum Pump [redacted] Volume flow rate 16m3/h Pressure<1x10-4	No.	1
7		Repair Kit for High Vacuum Pump Type: [redacted]	No.	4

3. You are requested to please give us your best FOB prices alongwith separate approx. air/sea freight charges upto Islamabad/Karachi, Pakistan respectively

4. An early reply will be highly appreciated.

With Best Regards

Figure 2.3. Copy of an inquiry for vacuum pumps and repair kits received by sales agents of the European manufacturer, later determined to have originated in Pakistan's gas centrifuge program.

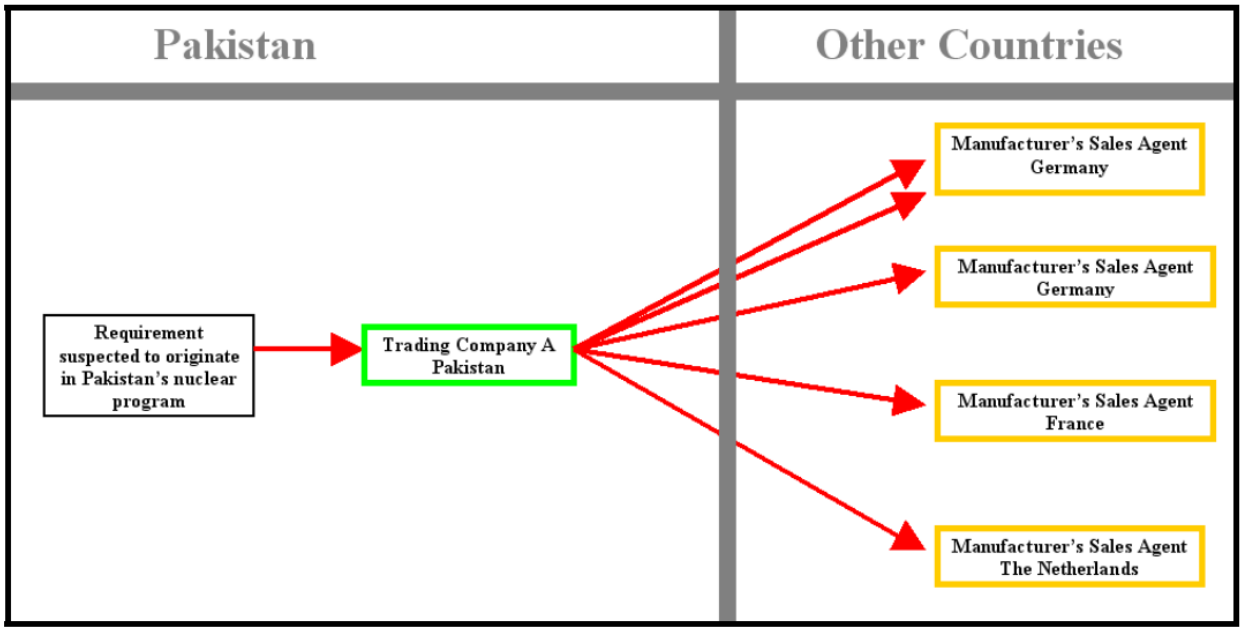
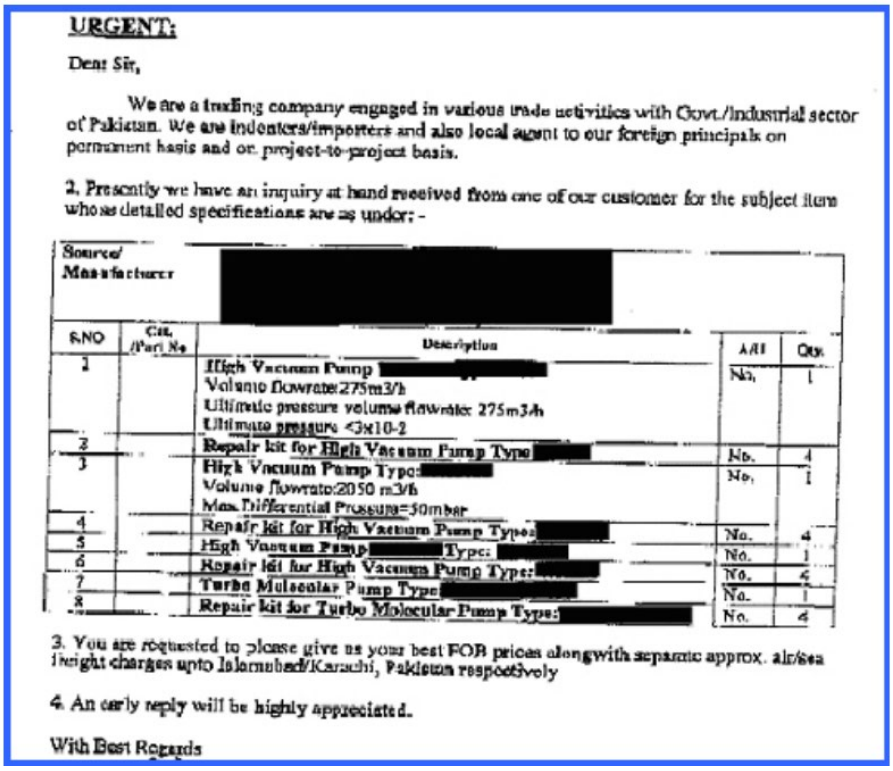


Figure 2.4. Path of inquiries sent to various sales agents of the European manufacturer.



URGENT:

Dear Sir,

We are a trading company engaged in various trade activities with Govt./Industrial sector of Pakistan. We are indentors/importers and also local agent to our foreign principals on permanent basis and on project-to-project basis.

2. Presently we have an inquiry at hand received from one of our customer for the subject item whose detailed specifications are as under: -

Source/ Manufacturer [redacted]

S.NO	Cat. /Part No	Description	A/U	Qty.
1		High Vacuum Pump [redacted] Volume flowrate:275m3/h Ultimate pressure volume flowrate: 275m3/h Ultimate pressure <3x10-2	No.	1
2		Repair kit for High Vacuum Pump Type [redacted]	No.	4
3		High Vacuum Pump Type: [redacted] Volume flowrate:2050 m3/h Max.Differential Pressure=50mbar	No.	1
4		Repair kit for High Vacuum Pump Type: [redacted]	No.	4
5		High Vacuum Pump [redacted] Type: [redacted]	No.	1
6		Repair kit for High Vacuum Pump Type: [redacted]	No.	4
7		Turbo Mulecular Pump Type [redacted]	No.	1
8		Repair kit for Turbo Molecular Pump Type: [redacted]	No.	4

3. You are requested to please give us your best FOB prices alongwith separate approx. air/sea freight charges upto Islamabad/Karachi, Pakistan respectively

4. An early reply will be highly appreciated.

With Best Regards

Figure 2.5. Copy of inquiry for various vacuum pumps and repair kits sent to sales agents of the European manufacturer, originating in Pakistan's gas centrifuge program.

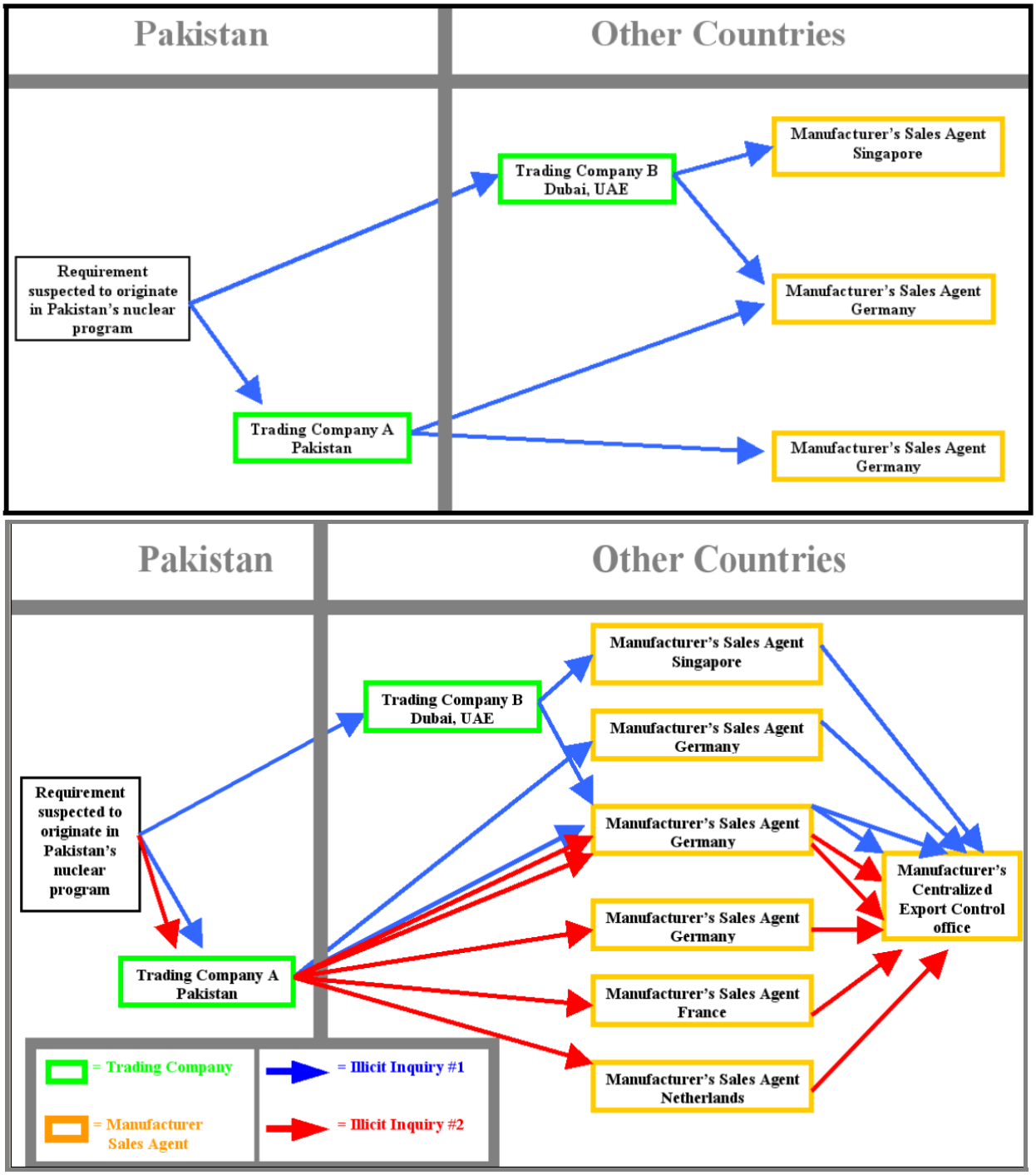


Figure 2.6. Paths of inquiries sent to various sales agents of the European manufacturer.

Upon receiving all the inquiries from their sales agents, the manufacturer's central export control office immediately recognized that the two trading companies were acting suspiciously. It instructed the sales offices not to fulfill the requests and notified authorities. Since the manufacturer's internal compliance system was centralized, where all suspicious inquiries received by sales offices were forwarded to a single export control office database at the manufacturer's headquarters, the full picture of the illicit procurement attempt came into

focus. All of the data on inquiries, illicit trading companies, and sales agents receiving the inquiries, were centrally collected. This central office functioned successfully as a detection hub with inputs from its sales agents, enabling detection of many potential illicit procurement attempts. Without this centralized internal compliance system, the sales agent in Singapore might not have known, for example, that Trading Company B had also sent an identical inquiry to another of the manufacturer's sales agents in Germany on the same day. The Singapore sales office might also have been unaware that Trading Company A had sent the exact same inquiry to another sales agent in Germany two days before.

Case 2.3: Large Quantities of Suspicious Vacuum Valve Orders from Iran[3]

Starting in August 2002, just before an Iranian opposition group revealed publicly the existence of the secret Natanz nuclear site in Iran, a European high-technology vacuum equipment manufacturer Leybold received a series of suspicious inquiries from trading companies for large numbers of small, fast-acting valves, called "microvalves," which it suspected were for use in Iran's then-secret uranium enrichment program. One type Iran was seeking in large quantities was Leybold's microvalve 28446, DN 10. These types of microvalves, however, were not on German or international export control lists, or even commonly believed to be of sufficient quality to be used in a gas centrifuge plant.

Over the next 14 months, Leybold received a total of 15 suspicious valve inquiries, five of which are depicted in Figure 2.7. This manufacturer specializes in cutting edge vacuum equipment, which has both nuclear and non-nuclear applications. The vast majority of the inquiries it receives are intended for legitimate and legal end-uses. A small fraction, however, originates from front companies seeking to illicitly purchase items for use in covert nuclear programs. The manufacturer's officials suspected that these valve inquiries were in the latter category. What they started to realize is that these inquiries revealed the nature and scope of Iran's secret gas centrifuge program months before the program was ever publicly revealed. Iran admitted to that program's existence in February 2003.

[3] David Albright, Paul Brannan and Andrea Scheel (Stricker), "A Company's Discretion Detects Large Iranian Valve Orders by Scrutinizing Items and End-Users Instead of Lists," *Institute for Science and International Security,* January 28, 2009, http://isis-online.org/uploads/isis-reports/documents/Iran_Valves_28January2009.pdf

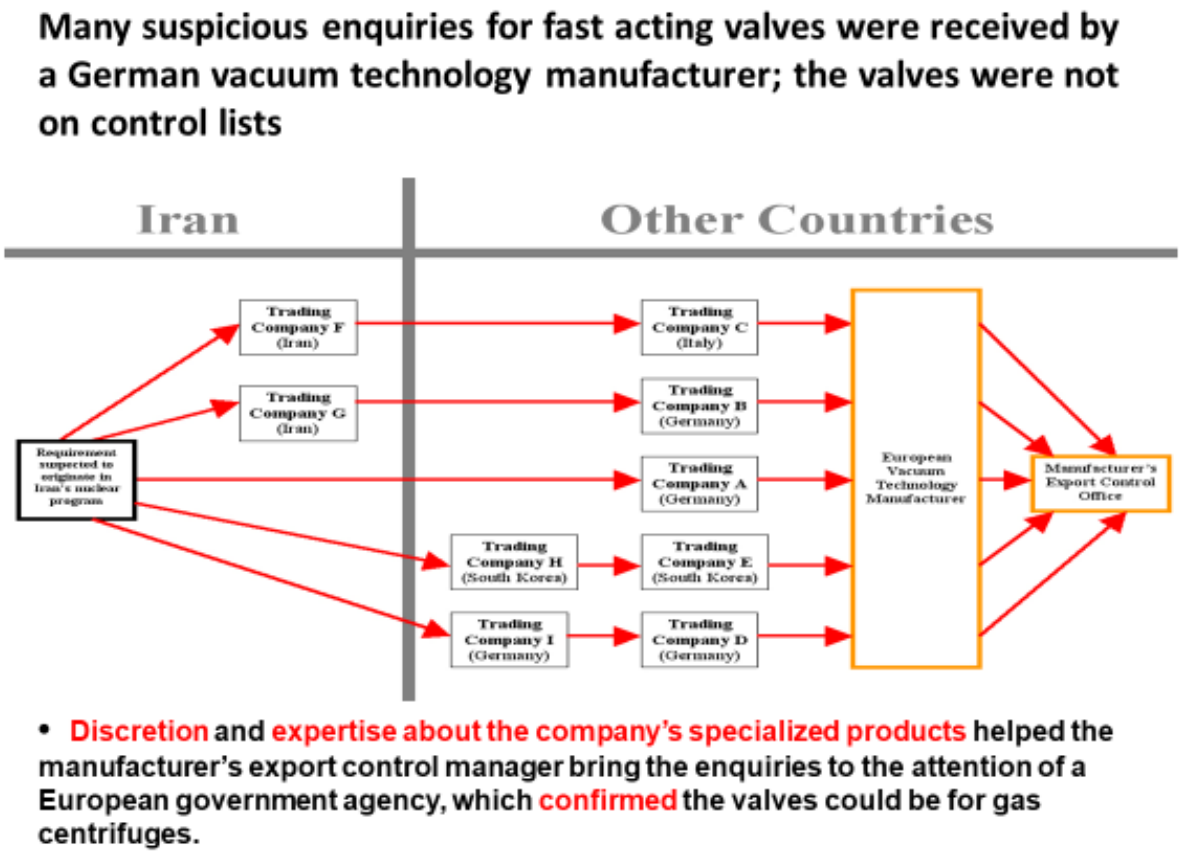


Figure 2.7. Diagram showing the path of five of the fifteen inquiries (also known as enquiries in European countries) for fast acting valves, received by Leybold, the German vacuum technology manufacturer, between August 2002 and October 2003. Export control managers for this manufacturer rightly suspected that these inquiries were intended for use in a gas centrifuge uranium enrichment plant in Iran.

Leybold received the first inquiry on August 14, 2002, from a German trading company (Trading Company A in the figure), which stated the valves were destined for a petrochemical factory in the United Arab Emirates. Leybold linked this company to Iran and did not make the sale. This inquiry was followed by another in October 2002 from another German company (Trading Company B), which stated that Iranian universities were the end-users, but the inquiry was for an initial 3,000 valves and a total of 50,000 valves, an unusually large number for a university. It was more in line with the requirements of a medium-sized gas centrifuge program of the type Iran was suspected of operating.

Other requests followed. In two more instances, Leybold received requests from German and Italian trading companies (Trading Companies C and D), which themselves were representing other trading companies, one of which was in Iran. The largest order, submitted in May 2003, was from a South Korean company (Trading Company E), seeking an annual quantity of 50,000 to 100,000 valves. The end-user of this request was an Iranian nuclear power plant, another

unlikely customer for this number of vacuum valves. The export control manager for Leybold at that time, Ralf Wirtz, had become convinced in 2003 that the orders were for the Natanz enrichment plant, which would need at least 150,000 fast-acting microvalves for all the centrifuges Iran planned to deploy. These centrifuge plants are based on an early Dutch design that Pakistan stole in the early 1970s, and later, that A.Q. Khan secretly sold to Iran in the 1980s and 1990s. This type of centrifuge, the P1, is subject to excessive vibration, and the fast-acting valves allow rapid shutdown of an individual centrifuge before it breaks. Three of these valves are needed per centrifuge, which is why so many would be needed in Iran's centrifuge plants at Natanz, and laterat another centrifuge plant called Fordow, located near Qom.

However, some were skeptical about stopping these sales, since the valves were not ones on German national or international control lists of dual-use items, which focus on such valves only if they are specially-prepared for use in a gas centrifuge uranium enrichment plant, which uses highly corrosive uranium hexafluoride gas. However, as the manufacturer's export officials had become more familiar with inquiries from sensitive countries, they noticed that proliferant states, which typically sought those specially-prepared valves, were deliberately avoiding ordering them, or were in general sidestepping ordering goods on lists of nuclear dual-use items subject to stricter licensing requirements in the most recent laws. Instead of ordering vacuum pumps and valves manufactured specially for gas centrifuge plants, which require export licenses, sensitive programs order the more generic non-controlled versions of the items from the manufacturer's catalogue, which are less reliable but can be used nevertheless. These items typically do not require an export license and requests are scrutinized by companies much less as to potentially unauthorized uses. In the above cases, the valves were not of the type found on lists of nuclear dual-use equipment that require a government-issued license to export. The procurement specialists and scientists running these programs had apparently learned that items on dual-use export control lists could be avoided by substituting items that were less capable, but still good enough for the intended nuclear purpose. Typically, they would break frequently, requiring more replacements. But these purchases would also attract far less scrutiny from suppliers and authorities; a strategy which apparently worked well until the early to mid-2000s.

In September 2003, Wirtz brought the inquiries to the attention of the German government agency responsible for export controls. This agency, after doing its own internal technical evaluation, confirmed Wirtz's hunch that these valves were suitable for use in a centrifuge plant and would not be approved for export to Iran. The inquiries continued through October 2003, at which point they stopped. Whether Iran succeeded in acquiring enough valves through other suppliers is unknown. But the inquiries had provided early warning of Iran's intentions to build thousands of centrifuges and valuable insight into the nature of the centrifuges.

Iran started ordering valves again from Europe in late 2005 or early 2006. Before authorities were aware, a British vacuum company sent an order of about 1,000 valves to Iran. Several similar inquiries followed for thousands of valves, fittings, and pipes that appeared to be enough for an entire facility. Several other vacuum companies received inquiries from a large

number of different trading companies. Initially, the orders came from a multitude of Iranian companies. Later, trading companies with offices in Dubai, and a company with offices in both Dubai and India, made similar orders. Iran's international search for valves became so apparent that the UN Security Council in 2006 highlighted valves in Resolution 1737, sanctioning Iran for refusing to suspend its uranium enrichment program and permit adequate International Atomic Energy Agency (IAEA) inspections.[4]

These actions spurred Iran to develop an alternative method of acquiring vacuum valves for its centrifuge program. Rather than ordering whole valves from abroad, it started to copy, or reverse-engineer, designs of vacuum valves and order from abroad only key subcomponents (see Chapter C.3). Once the orders were filled, an Iranian company would manufacture the vacuum valves in Iran using the imported parts. One associated location currently focused on the research and development activities on vacuum valves used for enriching uranium is reportedly in the support area of the Fordow enrichment plant.[5]

Case 2.4: Illicit Supply of Know-How and Training

Building nuclear facilities and weapons requires sensitive information, most of which is time-consuming and difficult to acquire. For many countries, acquiring this information through research and development programs is beyond their reach. Thus, many countries have sought short cuts, including through espionage and illicit purchase. This case discusses examples of the type of information Pakistan acquired in the 1970s as it sought to build gas centrifuges to make highly enriched uranium for nuclear weapons. It also gives an example of one country purchasing critical centrifuge information and training from the A.Q. Khan network in the late 1990s.

Theft and Proliferation of Sensitive Urenco Information

One of the greatest thefts of gas centrifuge enrichment technology occurred in the early and mid-1970s in the Netherlands from the uranium enrichment consortium Urenco and its subcontractors.[6] The perpetrator was Pakistan, which depended on the insider A.Q. Khan, who was then a trusted employee at a Dutch Urenco subcontractor. After returning to Pakistan in 1975, Khan eventually became the head of Pakistan's gas centrifuge program, where he continued to participate in the acquisition of sensitive information vital to the success of Pakistan's centrifuge program. Subsequently, he and his collaborators would sell this information to a range of buyers in Iran, Libya, North Korea, India, and elsewhere. Although this information is over forty years old and not commercially relevant today, it remains a proliferation threat. Moreover, modern methods of communication increase the potential

[4] *UN Security Council Resolution 1737 (2006),* December 23, 2006.
[5] "Iran Dismisses Rumors Fordow Nuclear Site is Closed, *Tehran Times*, July 20, 2019, http://www.tehrantimes.com/news/438359/Iran-dismisses-rumors-Fordow-nuclear-site-is-closed
[6] To learn more about this case, see Albright, *Peddling Peril* (New York: Free Press, 2010).

spread of this technology. Thus, responsible governments need to continue to guard against and track covert attempts to acquire these sensitive technologies.

Most of the Pakistani thefts occurred in 1974/1975 and were organized by Khan. Here, only a brief summary of the key purloined information is discussed:

- The drawings and specifications of the Dutch CNOR and German G2 centrifuges. These designs were subsequently spread by the Khan network and found by the International Atomic Energy in Iran, Libya, South Africa, Switzerland, and Malaysia.

- The research and development test results of the G-4 or 4-M centrifuges, which were second-generation German and Dutch centrifuges with an enrichment capacity of about double the G2 centrifuge, or almost ten separative work units per year per machine. Pakistan is believed to have developed these designs into a production-scale machine deployed at its enrichment plants. The Khan network spread these data to its node in South Africa for eventual transfer to Libya.

- Names of major suppliers, e.g. Leifeld, VAT, Leybold, Schenk, among others. This information spread widely.

- Safety studies for Urenco's commercial demonstration centrifuge plant, called E-21. This information was found in Iran.

Another batch of sensitive information was obtained in 1978/1979 by a group of Western contractors for Pakistan's centrifuge program, which by that time was building its first centrifuge plants near Kahuta, Pakistan.

- Uranium hexafluoride feed and withdrawal systems for the Dutch Urenco's demonstration plant B-21. This information was obtained principally by Gotthard Lerch. The Khan network subsequently spread it, and the IAEA found it in South Africa, Libya, and Switzerland.

- "Fast Acting" valve system for cascade protection during centrifuge failure (see Case 2.3 above). This information was obtained by Friedrich Tinner. It was subsequently found in Iran, Libya, South Africa, and Switzerland.

- B21 Plant Converter/Drive design, essentially the sophisticated motors and power supplies for the centrifuge. This information was acquired by Heinz Mebus and Gunes Cire; the latter organized the manufacture of centrifuge motor systems in Turkey. The IAEA subsequently found it in Turkey, South Africa, Iran, Libya, and Switzerland.

Although copies of these documents were recovered in Libya, South Africa, Switzerland, and Turkey following the busting of the Khan network in 2004, other copies exist, including in

Pakistan, Iran, and North Korea. Moreover, traffickers formerly involved in the Khan network may still have copies. Thus, a black market in these documents may still exist or emerge.

Training by the Three Tinners

Another way sensitive centrifuge information and expertise has spread is through covert training programs. An example is found in the evidence and statements from the three Tinners' trial in Switzerland in 2012. The "Three Tinners," namely the father Friedrich and his two sons, Urs and Marco, cooperated in the Khan network's international procurement network that was supplying Libya with a gas centrifuge plant. Overall, they made it possible for Libya to build uranium enrichment plants and produce weapon-grade uranium.

Toward that goal, they performed a variety of services as part of the supply of a turn-key gas centrifuge plant. In particular, they created a covert training center in Dubai, the Desert Electrical Engineering Factory (DEEF), to train Libyan technicians.

In 1998, Urs Tinner had moved to Dubai through the mediation of his father and worked there in furtherance of the Khan network's sales to Libya. While there, he served as DEEF's workshop manager. The Tinners performed the following services related to supplying a gas centrifuge plant to Libya:

- Procured machine tools and accessories for the training of Libyan technicians and supplied them to the DEEF;
- Produced and provided operating instructions and manuals for training purposes, which included translating them from English to German;
- Trained mechanics and technicians at the DEEF in:
    - basic mechanical skills of welding, turning, and milling related to a gas centrifuge plant;
    - vacuum and valve technology, including welding of bellows to end pieces for making bellows-sealed valves;
    - mass spectrometry;
    - working with centrifuge test modules;
    - assembling centrifuges and cascades;
    - operation of an enrichment plant;
    - electronic specialties
- Trained technicians and mechanics in the handling of uranium hexafluoride;
- Recreated technical drawings for the manufacture of P1 and P2 centrifuge components from "blueprints;" and
- Provided individual centrifuge-related lessons to the technical leader of the Libyan centrifuge program.

In order to provide training in the operation of gas centrifuge cascades, the Tinners manufactured test cascades, called modules 09 and 19, where the number refers to the number of centrifuges in the test cascade, and delivered them to the DEEF. In particular, they:

- Manufactured the test modules 09 and 19 and delivered them to the DEEF, including cooling systems for the condensation unit, measurement devices, leak detectors, sample containers, etc.;
- Ordered the P64 electronic control system for controlling the feed and withdrawal of a 64-centrifuge machine cascade, as well as parts of a 64-machine cascade in Switzerland, and supplied them to the DEEF;
- Manufactured storage containers of various sizes for holding enriched or depleted uranium hexafluoride and liquid nitrogen, as well as the appropriate special container valves, and delivered them to Dubai.

The Tinners also conducted training as part of providing goods related to the mass production of centrifuge components:

- Procured machine tools for the manufacture of gas centrifuge components in Turkey and a special mixer and vacuum oven for preparation of araldite for sealing of drive motors in the centrifuge and exported them to Turkey, and trained mechanics and engineers in Turkey;
- Procured the workshop equipment and production equipment for the Scope Company in Malaysia, thus machine tools and lathes for industrial mass production of centrifuge components, provided software to run the machine tools, and trained personnel at the workshop in the manufacture of centrifuge components;
- Manufactured P2 gas ultracentrifuges at Scope in Malaysia, procured raw material for their manufacture, as well as aluminum piping for the manufacture of P1 rotors, and shipped the finished parts to Dubai.

The Tinners also contracted with the Khan network to make 1,382 valves for the Libyan gas centrifuge plant. The Libyan plant was slated to hold a total of about 6,000 centrifuges in 38 cascades. On average, each cascade would have needed about 36 valves. The number and role of valves in Pakistani-type centrifuge cascades will be discussed further below.

Chapter 3. Deceiving Suppliers, Brokering, and Exploiting Weak Controls

This chapter focuses on five cases that involve the acquisition of a wide variety of dual-use goods by deceiving suppliers about their end-use or end-user. One case involves past brokering of goods for Iran's nuclear weapons program. Three of the cases involve China. China does not regulate the activities of companies effectively, and in many cases turns a blind eye in order to prioritize economic growth. Trading companies and brokers have been able to operate with near-impunity. As a result, countries such as Iran, North Korea, Syria, Pakistan, and past proliferant states have used China as a one-stop shopping hub to illicitly outfit their sanctioned weapons programs.

Case 3.1: Iranian Illicit Nuclear Procurement Network buys via a supplier's foreign subsidiary, with yet another intermediary involved[1]

Following tips from a European intelligence agency, a European company discovered a strategy used by Iran to circumvent export controls, in this case a clever scheme to obtain vacuum pump systems for its gas centrifuge program. The elaborate ruse involved a Chinese manufacturing company with an established relationship with the European company. In early 2006, this company received a tip from a friendly European government to be on guard for inquiries from Saudi Arabian companies for certain types of pumping systems that would be diverted to Iran. The company did not receive such an inquiry, but its South Korean subsidiary company did receive a similar inquiry from an entity wanting to ship such items to Iran. The company refused to make a sale.

Several months later, the European country's intelligence agency asked the company to look into a recent order placed by a suspicious Chinese company with its own Chinese subsidiary. After reviewing inquiries and contracts, the company found that the Chinese company had ordered 15 such pump systems, seven of which the company had already delivered via the European company's Chinese subsidiary. The Chinese company, an established manufacturing company, called an "original equipment manufacturer" (OEM), had ordered the pumps as part of a larger order the company had received to build oil purification equipment for electrical power plants. The supplier did not need its government's approval to supply the pumps; the sale did not require a license and was not overtly suspicious. The Chinese company had not previously been associated with illicit activities.

After the discovery, company officials from the European supplier immediately contacted the Chinese company and asked for the end-user of the equipment. The Chinese company official was vague. He said that the vacuum equipment, including the pump systems, was for an overseas customer, and in fact the firm had already exported the seven pump systems, but he refused to reveal the customer. The European company stopped further shipments of pumps

[1] Case information provided by an anonymous European vacuum equipment manufacturer.

to the company. The Chinese company demanded the rest of the pumps or all its money back. Then, it cancelled the order, perhaps to prevent having to admit at some stage that its actual customer was Iran.

European government authorities were notified, one of which learned from the Chinese government that the pumps did indeed go to Iran. Although they did not learn the exact end-user, they believed Iran's centrifuge program was the likely customer. Figure 3.1 shows this scheme.

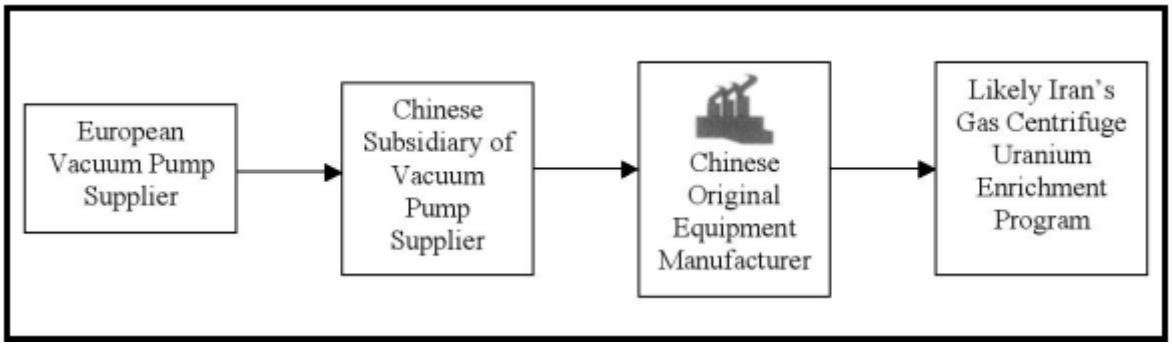


Figure 3.1. Diagram showing the vacuum pumps sold to Chinese manufacturer from European supplier. The Chinese manufacturer then sent the pumps to Iran where it is believed they were utilized by Iran's gas centrifuge program.

No prosecution by its government was launched against the European company for its export of the pumps. Instead, the intelligence service applauded the European company's cooperation to uncover a new Iranian scheme. The government's attitude was that companies should not be punished for exercising good citizenship. They detected an illicit procurement scheme later and then tried to help prevent further damage.

This case highlights the importance of governments cooperating with companies on suspected illicit procurement attempts. If the European authorities had not contacted the European supplier to inform it about a new Iranian illicit procurement scheme, the supplier would have never known that the vacuum pumps were sent to Iran and likely ended up in its gas centrifuge uranium enrichment program. Even the best internal compliance system cannot detect these types of illicit procurement attempts, and cooperation between government and industry is necessary in order to prevent smuggling networks from succeeding.

Case 3.2: Fake Defense Contractor Indicted for working inside the United States to export military-related drawings to Turkey[2]

On September 5, 2018, the owner of a New Jersey defense contracting firm was indicted by a grand jury of the U.S. District Court in the District of New Jersey on charges of wire fraud, conspiracy to commit wire fraud, violating the Arms Export Control Act (AECA), and conspiracy to violate the AECA.[3] Ferdi Murat Gul, a Turkish citizen, was the principal owner, chief executive officer, and general manager of two U.S.-based businesses: an alleged defense contracting company, Bright Machinery Manufacturing Group Inc. (BMM), and an alleged manufacturing company, Ferdi Murat Gul Machinery Group (FMG), and also held ownership interests in a manufacturing company in Turkey, HFMG Insaat (HFMG).[4]

From October 2010 to June 2015, BMM was awarded approximately $7 million in 346 U.S. Department of Defense (DOD) Defense Logistics Agency (DLA) contracts to manufacture military parts in the United States and provide them to DOD customers, such as the Army, Navy, Air Force, Marine Corps, and Coast Guard. But according to the indictment, in reality, BMM was a front company set up with the purpose of defrauding the United States. The parts it manufactured included those "for torpedoes for the U.S. Navy, bomb ejector racks and armament utilized in U.S. Air Force aircraft, and firearms and mine clearance systems used by U.S. military personnel abroad." [5] Allegedly, Gul and two unnamed, un-indicted co-conspirators falsely claimed that BMM manufactured these parts in the United States. However, the indictment alleged that BMM illegally exported technical military drawings to manufacture the parts in Turkey, and then sold the parts – some of which had "design flaws and non-conformities and were unusable" – to U.S. customers.[6]

One of Gul's co-conspirators, a U.S. citizen, served as the contracts' primary point of contact and apparently went through government-mandated certifications to register BMM as a U.S. contractor. Gul and his two co-conspirators allegedly forged documentation and certifications to falsely represent BMM as a U.S. domestic manufacturer. This meant that all military parts supplied by BMM had to be "Domestic End Products," or 50 percent of the total cost of parts had to be comprised of components mined, produced, and manufactured in the United States. As a foreign contractor, HFMG was "only permitted to supply 'Qualifying Country End Products'

[2] Hanah Joudi and Andrea Stricker, "Case Study: Fake Defense Contractor Indicted for Exporting Military Related Drawings to Turkey," *Institute for Science and International Security,* September 25, 2018, http://isis-online.org/uploads/isis-reports/documents/Case_Study_Gul_Network_25Sept2018_Final.pdf

[3] U.S. Department of Justice, Press Release, "Owner of Defense Firm Charged with Conspiracy to Defraud Department of Defense of $7 Million, Violate Arms Export Control Act," September 6, 2018, https://www.justice.gov/usao-nj/pr/owner-defense-firm-charged-conspiracy-defraud-department-defense-7-million-violate-arms

[4] United States District Court in the District of New Jersey, *Indictment: United States of America v. Ferdi Murat Gul, a/k/a "Fred Gul,"* September 5, 2018, Available at: https://www.justice.gov/usao-nj/press-release/file/1092036/download

[5] "Owner of Defense Firm Charged."

[6] Ibid.

(i.e. foreign-made products) from Turkey to U.S. vendors." It was not permitted to supply Domestic End Products.

Gul was charged with falsely representing the location of BMM's manufacturing operations to obtain contracts with the DOD and exporting and conspiring to export technical military drawings to Turkey without a license. The AECA "prohibits the export of defense articles and defense services without first obtaining a license from the U.S. Department of State."[7] Gul faces a maximum penalty of 20 years in prison and a $250,000 fine for each wire fraud count, and another 20 years in prison and a $1 million fine for each AECA violation, if apprehended. U.S. authorities believe Gul is at large in Turkey. It is not known whether Gul transferred the U.S. military part drawings to others.

Case 3.3: A Broker's Procurement of Equipment likely for Iran's nuclear weapons program[8]

In November 2007, German authorities arrested a German-Iranian citizen, Mohsen Vanaki, on suspicion that he illegally brokered the transfer of dual-use equipment to Iran with applications in nuclear weapons programs.[9] In an apparent attempt to hide the equipment's end-users, Vanaki's small German trading company arranged the sale of dual-use nuclear and military equipment from Russian, European, and American manufacturers to Iranian front companies located in the United Arab Emirates.[10] In a surprise move, Vanaki's defense attorneys cited U.S. intelligence findings claiming that Iran did not have a nuclear weapons program at the time of the alleged crime as evidence of their client's innocence. Vanaki's firm maintained a commercial relationship with a Tehran-based company, Kimya Pakhsh Sharg Co. Ltd., referred to as only "K. Co. Ltd." in German court documents. Aryadaran General Trading LLC in Dubai, Electroniat Shamsal Sahra Co., and Modern Technologies either served as UAE-based front companies for Kimya Pakhsh Sharg or made payments to Vanaki on its behalf. According to court documents, Kimya Pakhsh Sharg obtained nuclear and military goods for Iran by circumventing trade restrictions using front companies and phony end-use declarations. Vanaki had direct contacts with the Iranian company's director and an employee, referred to in German court documents as "Dr. N." and "Ka.," respectively. Vanaki appears to have had a long history of supplying Iranian military entities. In the 1990s, he reportedly supplied Iran's Defense Industries Organization.[11]

On June 26, 2008, Vanaki was officially charged with one violation of the German War Weapons Control Act and two violations of the Foreign Trade and Payments Law, which are

---

[7] Ibid.

[8] David Albright and Christina Walrond, "The Trials of the German-Iranian Trader Mohsen Vanaki: The German Federal Intelligence Service Assesses that Iran Likely Has a Nuclear Weapons Program," *Institute for Science and International Security,* December 15, 2009, http://isis-online.org/isis-reports/detail/the-trials-of-the-german-iranian-trader-mohsen-vanaki-the-german-feder/8

[9] *Beschluss*, Bundesgerichtshof, March 26, 2009 (Decision of the Federal Court of Germany).

[10] "Germany holds man over classified exports to Iran," *Deutsche Presse Agentur*, November 29, 2007.

[11] Andreas Ulrich, "Motor im Handgepäck," *Der Spiegel*, December 3, 2007.

antiproliferation laws designed to control the development, production, or trade of goods that could aid weapons of mass destruction programs in countries of proliferation concern. Though the War Weapons Control Act also applies to conventional weapons, the harshest penalties are reserved for offenses concerning the proliferation of materials for chemical, biological, or nuclear weapons programs.[12] Under the Foreign Trade and Payments Act, the brokering of material for a nuclear weapons program is of particular concern because it threatens the foreign relations and external security of Germany.[13]

Vanaki brokered for Iran the sale of two high-speed cameras that have important applications in nuclear weapons programs.[14] According to court documents and interviews with knowledgeable German officials, he tried to purchase through another German firm a large number of American-manufactured specialized radiation detectors modified to withstand a harsh environment, which court documents described as "nuclear detonation effects." The German company, Karl Steiger GmbH, however, cancelled the order because it could not obtain sufficient information about the equipment's end use to secure German government approval for the export.[15] Vanaki also allegedly tried to arrange the sale of night vision goggles from a Swiss manufacturer to Kimya Pakhsh Sharg, but Swiss authorities also found the stated end-user information to be suspicious.

Surprising Use of U.S. National Intelligence Estimate

Mohsen Vanaki's trial was originally set for the summer of 2008 before the German Oberlandesgericht of Frankfurt am Main (a Hessian state court). A critical issue for this court was whether Iran had a nuclear weapons program. Convicting Vanaki under the War Weapons Control and Foreign Trade Acts depended on the court finding it sufficiently likely that the country receiving the equipment brokered by Vanaki was developing nuclear weapons at the time of the alleged crime. In a surprising decision, the Oberlandesgericht in August 2008 dismissed all charges against Vanaki, basing its decision largely on the U.S. intelligence community's 2007 *National Intelligence Estimate (NIE)* on Iran. The majority of the NIE is classified, but a short, declassified summary is available. The following are several key judgments of the NIE from that summary:

- We *assess* with high confidence that until fall 2003, Iranian military entities were working under government direction to develop nuclear weapons.
- We *judge* with *high confidence* that the halt lasted at least several years. (Because of intelligence gaps discussed elsewhere in the Estimate, however, the DOE [Department of Energy] and the NIC [National Intelligence Council] *assess* with only *moderate*

[12] *The War Weapons Control Act of Germany,* Amended October 11, 2002.
[13] *Foreign Trade and Payments Law of Germany,* Amended March 28, 2006.
[14] "Beschluss" and "Motor im Handgepäck." See: "German-Iranian Accused of Arranging Illegal Business Deals with Iran," BBC News, June 28, 2008. At least one of the cameras was capable of one million frames per second, far above the level that triggers export controls.
[15] "German-Iranian Accused of Arranging Illegal Business Deals with Iran."

confidence that the halt to those activities represents a halt to Iran's entire nuclear weapons program.)

- We *assess* with *moderate confidence* Tehran had not restarted its nuclear weapons program as of mid-2007, but we do not know whether it currently intends to develop nuclear weapons. (italics added)

The court focused on the third finding, ruling that Iran was probably not developing nuclear weapons at the time of the defendant's alleged crime and dismissing the charges against Vanaki, even though, based on German intelligence about suspicious procurements made by Iranian military entities and other evidence, according to a knowledgeable German official, Germany's intelligence agency assessed that there were strong indications that Iran had a nuclear weapons program at the time of the crime. In reaching its decision, the court mischaracterized the assessment provided by the Bundesnachrichtendienst (BND), Germany's foreign intelligence service, as "extremely vague." Today, the 2008 BND assessment is strengthened by newly available information from the Iranian Nuclear Archive, a portion of which was seized by Israel in early 2018, showing a potential continuation of Iran's nuclear weapons-related activities.[16]

Overturned on Appeal

German federal prosecutors appealed the judgment to the Bundesgerichthof, Germany's Federal Court of Justice. The federal judges decided on March 26, 2009, that the Oberlandesgericht, the state court, should not have dismissed the findings of the BND. They ruled preliminarily that at the time of the crime, Iran probably had a nuclear weapons program. The federal court rejected the lower court's characterization of the BND's statement as extremely vague. Its decision stated that the Oberlandesgericht failed by overstretching requirements for the admission of additional information or intelligence. For the appeals hearing, the BND provided the federal court with a supplementary report containing additional evidence. This report discussed Iran's development of a new missile launcher and the similarities between Iran's procurement efforts and those of countries with known nuclear weapons programs, such as Pakistan and North Korea. The federal court ordered a retrial of Vanaki under the original charges at the Landgericht, a German district court below the Oberlandesgericht, and instructed the district court to take into consideration the findings of the BND and other available evidence about the likelihood of Iran having had a nuclear weapons program at the time of the alleged crime.[17]

Although the German federal judges did not seek to decide on Vanaki's guilt or innocence, in order to overturn the decision of the Oberlandesgericht, they had to find it sufficiently likely that the accused would be convicted in a retrial. Therefore, the likelihood of Vanaki's conviction depended on the judgment that Iran was probably developing a nuclear weapons

[16] For detailed information on the Nuclear Archive, see the Institute's web site, www.isis-online.org.

[17] The federal court, at the request of the federal prosecutors during the appeal, dismissed a third charge because it had little "weight" compared to the other two alleged violations (see section on night vision goggles below).

program at the time of the alleged crime. The decision legally defines "developing" as all measures taken to create the technological conditions for producing nuclear weapons, including the planning and construction of nuclear weapon production facilities. The Bundesgerichtshof stated that the Oberlandesgericht's use of the NIE in its decision was inappropriate. It ruled that other evidence that merits consideration offsets the NIE's findings. The Oberlandesgericht had overemphasized in its judgment the finding of the NIE about the status of Iran's nuclear weapons program and improperly downplayed the BND's findings. The Oberlandesgericht correctly recognized that the BND's assessment did not contain proof of an Iranian nuclear weapons program, but it failed to recognize that the NIE's judgment about the program was also not proof. According to the NIE, "In all cases, assessments and judgments are not intended to imply that we have 'proof' that shows something to be a fact." In addition, the use of the term "moderate confidence" in the NIE carries with it a significant level of uncertainty about the judgment that an Iranian nuclear weapons program did not exist in 2007.

Major Equipment Obtained or Sought by Vanaki

High-speed Cameras. In April 2007, according to the Bundesgerichtshof's decision, a front company of Kimya Pakhsh Sharg submitted a request for two sophisticated high-speed cameras to Vanaki's firm. According to the federal court's statement, Vanaki might have known that the cameras were for Iran's nuclear program. By his own admission, Vanaki knew of the possible military uses of the cameras. The federal court also asserted that he acted deliberately in breach of the embargo with Iran and contributed significantly to the complex, conspiratorial way in which the cameras were delivered to Iran. Vanaki acquired the cameras from the Moscow-based manufacturer Bifo Company, naming the end-user as a university in the Middle East. The model numbers of the two cameras were K008 streak and "uniframe" camera and K011 "nineframe" camera. He sent a price-quote to Kimya Pakhsh Sharg that stipulated his commission as 30,630 € ($41,996.79 in 2007 USD), implying a high sales price for the cameras since commissions are typically approximately five to ten percent. Vanaki allegedly visited Iran on a number of subsequent occasions to finalize the details of the transaction.

The cameras traveled from Russia to Iran before November 1, 2007, without the involvement of the German authorities to ensure export was legal. The Russian government appears to have done little, if any, scrutiny of this sensitive dual-use export. The high-speed cameras brokered by Vanaki are designed to take a rapid series of pictures and are used to photograph high-speed events that could have civil or military applications. Bifo's logo (Figure 3.2) contains pictures of lightning and a mushroom cloud, illustrating two important applications of its products. According to an Institute analysis, Iran would likely use these high-tech, high-specification fast cameras in its sophisticated military development programs that study high-speed events, including high explosive testing. In a nuclear weapons program, these cameras are capable of a range of uses involving the detonation of high explosives as part of compression tests associated with nuclear weapons development or the initiation of the nuclear explosion. The

use of high-speed cameras in Iran's nuclear weapons program has been documented in the Nuclear Archive.[18]

Figure 3.2. Bifo Logo, file name of this picture on www.bifocompany.com is boom.jpg

The Bifo company has links to Russia's nuclear weapons program. Bifo was founded by the State All-Russian Research Institute for Optical and Physical Measurements, VNIIOFI. Scientists from this company gave their affiliations as both VNIIOFI and Bifo. They published occasionally with scientists from the All Russian Research Institute of Experimental Physics, VNIIEF, which is well-known as the first nuclear weapons laboratory in the former Soviet Union, the organization that developed the first Soviet nuclear device and many generations of nuclear weapons thereafter. The topics of joint papers are directly related to nuclear weapons development or other high-speed phenomena related to explosives and shock waves. The Institute learned that Iran pursued additional contacts with Bifo (see Chapter C.6).

Radiation Detectors. In May 2006, Vanaki received a request from Kimya Pakhsh Sharg for a number of components of U.S. manufacture, including an order for about 100 individual neutron, beta, and gamma detectors modified for a harsh environment and designed for the measurement of high levels of radiation, according to a knowledgeable German expert. Based on the manufacturer's specifications, the detectors could be used for military purposes. To obtain the detectors, Vanaki contacted Karl Steiger GmbH in Mannheim, labeled "St. GmbH" in the court records, which in turn requested the items from a United States manufacturer, called "L." The firm designated an end user in Dubai at the request of Vanaki. The German firm agreed to purchase the detectors. Vanaki then quoted the purchase price to Kimya Pakhsh Sharg as 87,245.40 € ($109,606.40 in 2006 USD). Karl Steiger GmbH received this sum in three installments.

In May 2007, Karl Steiger GmbH submitted to the Federal Office of Economics and Export Control an export license application for the radiation detectors. This application required an end-user certification and a detailed customer profile. According to the Bundesgerichtshof's decision, Vanaki and Ka. at Kimya Pakhsh Sharg decided to falsify this information and attempted to fabricate an end-user in Dubai in order to hide the fact that Kimya Pakhsh Sharg

[18] See for example, David Albright and Olli Heinonen, "Shock Wave Generator for Iran's Nuclear Weapons Program: More than a Feasibility Study," *Institute for Science and International Security,* May 7, 2019, http://isis-online.org/isis-reports/detail/shock-wave-generator-for-irans-nuclear-weapons-program-more-than-a-feasibil/8

was the actual recipient. The Federal Office of Economics and Export Control asked Karl Steiger GmbH for additional information about the purpose of the export. Vanaki and Ka. conferred to determine what intended purposes would be most plausible to the licensing authorities. Vanaki preferred to offer a false end use in agriculture or medicine, but Ka. ultimately decided to use the cover story that, despite the detectors' potential application in a nuclear plant, they would be used in the cement industry. However, the licensing authorities continued to raise questions with the German firm. In late summer, Vanaki's contact at Karl Steiger GmbH informed him that without additional information about the end-use of the equipment, his company could not provide the goods. Despite many subsequent attempts, Vanaki could not reach his contact at Karl Steiger GmbH to provide adequate information, and the German firm terminated the agreement. Vanaki was unsuccessful in returning the funds to Kimya Pakhsh Sharg.

Night Vision Goggles. In May 2007, a front company of Kimya Pakhsh Sharg requested 20 night vision goggles from Vanaki's firm. Vanaki contacted a Swiss manufacturer about buying the goggles; however, the transaction was not completed because the Swiss regulatory export authority determined the end-user information to be insufficient. Vanaki was also charged with a violation of the German Foreign Trade and Payments Law for attempting to secure the export of night vision goggles. However, at the request of the federal prosecutors, the Bundesgerichtshof, or federal court, dismissed this charge, stating this violation had relatively little weight compared to the other allegations. If convicted on this count, Vanaki would likely have received only a fine, whereas a conviction on the other charges would result in a sentence of imprisonment.

Other Equipment. Vanaki provided a range of other items to Iran. He is reported to have sold Iran vacuum pumps. Police investigators also found records of an additional dozen procurements on Vanaki's laptop, which authorities seized during their investigation. It was unclear from these records, however, whether the items were successfully sent to Iran. None of the items mentioned on the laptop were prominent nuclear dual-use equipment.

Retrial in September 2009

The retrial of Mohsen Vanaki began on September 11, 2009 in the district court of Frankfurt (Landgericht). On September 24, the district court ruled against Vanaki. Based on this testimony, the district court found that Vanaki should have been aware that the items he sought to procure for Iran could be used in a nuclear weapons program. Vanaki was sentenced to a 22-month suspended sentence and ordered to pay the court 5,000 Euros ($7,300).

Case 3.4: Shenyang Machine Tool Company's illicit sales to North Korea[19]

A relatively large Chinese company, Shenyang Machine Tools Company, allegedly supplied sophisticated machine tools to North Korea in violation of supplier country trade control laws, according to government sources. The exports allegedly occurred in 2015. Although Shenyang company officials stated that the exports were inadvertent, other evidence suggested that the company did know or should have known that the end destination of the controlled goods was North Korea. The Chinese government refused to cooperate with foreign criminal investigations to determine the actual situation, backing the company's claim that the exports were inadvertent or uncontrolled re-exports. Complicating matters, supplier countries were hesitant to share details about potential illegal re-exports with China because of China's history of lax enforcement and cover-ups of such cases. As a result, legal options to investigate the company's exports have been limited.

Shenyang Machine Tools Company, headquartered in the city of Shenyang in northeast China, is a large company that sells a wide range of machine tools, some highly sophisticated. The machine tools use a range of subcomponents imported from major Western supplier nations. It sells its machine tools in China and globally, including in Europe and the United States. It also supplies the Shenyang Aircraft Company, which builds both military and civilian aircraft.

European government officials gathered evidence that at least two 6-axis machine tools, containing controlled, imported subcomponents, were exported to North Korea in about 2015 without authorization from the supplier country, a requirement of the original supply of the goods. In short, the re-export was banned unless it had the approval of the European government. The European country decided to investigate the responsible individuals at the Shenyang company, but this effort failed due to lack of Chinese government cooperation.

The subcomponents at issue were from a shipment of control units and software licenses for 6-axis machine tools. The goods are on the lists of the NSG, Missile Technology Control Regime (MTCR), and other control lists. These goods were supplied to Shenyang Machine Tools under the condition that they would not be retransferred to North Korea or other sanctioned states.

Shenyang Machine Tools has strong ties to North Korea. For example, it hosted a North Korean delegation in October 2013. Evidence indicates that at the time of the re-exports it employed a person whose sales area was stated to be North Korea. Shenyang Machine Tools Company officials claimed that the exports at issue were inadvertent. However, the assertion is contradicted by evidence obtained by the exporting country.

It is true that Shenyang, located approximately 250 kilometers from North Korea, has a large North Korean population. As has happened in China before, North Koreans based in China seek goods for North Korean WMD, missile, and military programs, posing as legitimate buyers

[19] Albright, "Shenyang Machine Tools Company," *Institute for Science and International Security,* April 13, 2017, http://isis-online.org/isis-reports/detail/shenyang-machine-tools-company/

pretending to use the goods within China but instead smuggling them to North Korea. However, this case was different. The evidence indicated that company officials knew the end-user of the controlled machine tools was North Korea.

The evidence gathered by the Western government further established that Shenyang Machine Tools Company and its sales agents also lacked effective, robust internal compliance programs (ICPs) that can provide assurance to international suppliers that the machine tools of Shenyang Machine Tools are not being diverted to North Korea. This assurance is particularly important today because of the tightened UN Security Council resolutions that ban exports to North Korea's proliferation programs.

As this case highlights, China has been hesitant to enforce its own trade control laws or UN Security Council resolutions on North Korea. This non-compliance is a product of poor awareness among Chinese industries, underdeveloped domestic trade control and sanctions legislation, and a lack of political will in the government to enforce laws that could be detrimental to economic growth. It also highlights the need for Western governments to more carefully scrutinize controlled exports to Chinese companies, such as Shenyang Machine Tools Company, obtain verified assurances from these Chinese companies that the controlled goods will not be re-exported without approval, and launch criminal investigations when violations are detected.

Case 3.5: North Korea's Procurements in China for a plutonium-production nuclear reactor

As is well-known and illustrated in other case studies, the North Korean government directs highly organized and centralized illicit trade efforts to outfit its nuclear programs. The government also uses North Korean government officials stationed at embassies to conduct illicit procurement-related business and recruits private companies to obtain goods. Moreover, North Korea has established entities abroad under its control that seek goods. In addition, it uses North Koreans residing abroad who own private companies in that country.

For many years, North Korea has been active in China and Hong Kong seeking goods for its nuclear programs. North Korean entities contract with private Chinese and Hong Kong trading companies and sometimes manufacturing companies to acquire these goods, either from Chinese suppliers or subsidiaries of Western or Japanese suppliers in China.

Since 2009, North Korea has procured goods for renovating its small gas-graphite reactor at the Yongbyon nuclear center, typically called the 5 megawatt-electric (MWe) reactor. This type of reactor is aged and typically uses rather archaic, not overly sophisticated equipment. However, North Korea has bought a range of goods abroad for this reactor. It decided to restore and upgrade this old reactor, which started in 1986, likely because it is North Korea's only source of plutonium for nuclear weapons. North Korea either cannot make these goods or believes foreign acquisition is more economical and provides higher-quality goods.

The items North Korea procured were not specially produced for nuclear reactors and were not particularly sophisticated dual-use goods. Examples of its procurements in China for the 5 MWe reactor include:

- Carbon dioxide blowers for the reactor's primary cooling system which uses carbon dioxide as the coolant;
- A Japanese emergency generator;
- Sulzers water pumps for the secondary cooling system, which uses water, and is subsequently discharged into the adjacent river; and
- A special aluminum-magnesium powder for making cladding of fuel for this reactor. This cladding is available from a single British company. Britain developed this type of gas-graphite reactor and still has a few operating.

North Korea also sought equipment in Europe in the mid-2010s to extract carbon dioxide during urea fertilizer production and store it underground. The carbon dioxide in the primary coolant system of the 5 MWe reactor needs periodic replenishment. Urea fertilizer production requires huge amounts of carbon dioxide produced by burning anthracite. Typically, the excess carbon dioxide is not captured, but in one thwarted attempt, North Korea sought, rather cleverly, to buy carbon capture equipment, valued at millions of dollars. The equipment looked to be, on the surface, to be for a type of "green initiative" to reduce carbon dioxide emissions at a major urea fertilizer production plant, called the Namhung Youth Chemical Complex Fertilizer Factory. Just prior to the approval of the export, governmental non-proliferation experts objected to the sale, arguing that a key use was likely for capturing carbon dioxide for the 5 MWe reactor. Despite this proliferation success, based on commercial satellite images of the 5 MWe plant, trucks holding tanks of carbon dioxide have appeared periodically, adjacent to the reactor, so North Korea must still have a way to produce carbon dioxide for this reactor.

Because of sanctions and strategic trade controls, North Korea would never be able to obtain permission to purchase equipment for the 5 MWe reactor, an unsafeguarded producer of plutonium for nuclear weapons. As a result, North Korea buys what it needs principally in China, apparently avoiding specially-prepared equipment for nuclear reactors that would be subject to intense scrutiny by export authorities.

Chapter 4. Undercutting Controls: Proliferant States' Duplication of Pressure Transducers

Iran, North Korea, Pakistan, and other states proliferating nuclear weapons have sought a specialized device, a pressure transducer, internationally and illegally by the thousands. Pressure transducers are difficult to manufacture, but are critical devices used to measure the pressure in the vacuum systems of gas centrifuge plants. Assisting their illicit efforts, China now appears to have a domestic capability to produce pressure transducers, following efforts to reverse-engineer Western items. At least one proliferant state, namely Iran, is also increasingly creating its own capacities to build these devices in order to reduce dependence on importing this vital equipment needed for uninterrupted operation and anticipated expansions of gas centrifuge plants. However, both the Chinese and Iranian efforts likely depend on obtaining subcomponents of pressure transducers from Western suppliers.

Pressure transducers are difficult to produce reliably, which has forced countries with secret or sanctioned gas centrifuge plants to procure them from abroad illicitly, often at great risk of prosecution by supplier countries such as the United States. Iran, for example, has needed to illicitly import thousands of them in order to operate its Fordow and Natanz enrichment plants (see Chapter 11). Many are made in the United States and subject to strategic trade controls as well as Iran sanctions. In the past, Pakistan acquired many U.S.-made pressure transducers. North Korea may have acquired U.S.-made pressure transducers as well, utilizing the same Chinese conduit as Iran. In addition, more recently, Pyongyang has also bought pressure transducers from a Chinese manufacturer.

Several countermeasures, including improved sanctions, reformed internal corporate controls, and successful U.S. government prosecutions, such as of Chinese nationals involved in illicit commodity trafficking schemes, have complicated proliferant states' overseas purchase of pressure transducers. These controls have even served as a form of a brake on enrichment programs as they encountered difficulties in obtaining enough pressure transducers. The resulting scrutiny of such procurements has also served as a telescope into the status and scope of centrifuge programs, much of which is often secret. However, this brake may no longer hold given the ability of China to make and sell pressure transducers and growing efforts of countries to build their own.

Given that pressure transducers break frequently, and a steady supply is critical to the operation of gas centrifuge plants, it is unsurprising that countries have sought to establish indigenous production capacities. However, they will likely need to continue importing critical subcomponents of pressure transducers, some of which may be controlled on suppliers' nuclear dual-use lists and would require a license for export. It is therefore critical for governments and suppliers to remain aware of this trend, find better ways to determine if these purchases are occurring secretly, and prioritize preventing such illicit procurements.

Case 4.1: Domestic Chinese Pressure Transducer manufacturing company sells to North Korea and perhaps Iran

According to a member state's documents provided to the UN Panel of Experts on North Korea, Kang Mun Kil, designated for nuclear procurement activities by Resolution 2270 (2016), bought pressure transducers for North Korea at least twice in 2013 and 2016.[1] The documents show that Kang Mun Kil procured these pressure transducers from a Chinese company, Shanghai ZhengTai Instruments Co., Ltd, aka Zhen Tai Instruments. The sale reportedly appeared as a domestic sale in China, meaning the goods were sold from one Chinese company to another. North Korean agents, secretly behind the procurement, then reportedly transported the goods illegally to North Korea. How much ZhengTai company officials knew is publicly unknown.

This report is significant since Chinese companies have not previously succeeded in producing high-quality pressure transducers able to compete with those produced by such companies as MKS Instruments, the major pressure transducer supplier headquartered in the United States, and a few other Western brands (see Chapter 11). Previously, MKS and other brands of pressure transducers had ended up in the centrifuge programs of Iran, India, Pakistan, and North Korea. It appears that as MKS and other Wester suppliers were tightening their controls, Shanghai ZhengTai managed to learn to make adequate ones and was selling them to North Korea and possibly Iran's gas centrifuge programs.

According to the UN Panel's 2019 report, "Shanghai Zhen Tai has also been advertised as an exporter of vacuum equipment to the Democratic People's Republic of Korea on a commercial website."[2] A section of Shanghai Zhen Tai's website, "Company Overview" (accessed in 2017 and 2019), discussed its CPCA series of pressure transducers, stating (translated from Chinese):

> *With ZhengTai CPCA series of capacitance diaphragm vacuum absolute pressure transmitters, ZT is very proud of gaining a Silver Medal of State Science & Technology Achievement Award issued by China Nuclear Industry Ministry (CNUM) and being qualified as a CNIM listed vendor. Because of its outstanding performance, solid stable quality, and excellent services, ShengTai CPCA series has been sold not only nation wide in China, but also to Southeast Asia, Korea, Russia, and USA*.

Iran's centrifuge program may have learned about this company in Shanghai as early as 2009 (see Chapters 11 and C.4). Its constant concern was finding a safe supply of high-quality pressure transducers for its the centrifuge plants, a problem compounded by their essentially perishable nature.

The UN Panel reported that Kang Mun Kil used a Hong Kong company, "Y Y Shun Limited," for procurement activities. Further, according to the Panel report:

---

[1] UN Security Council, *Report of the Panel of Experts established pursuant to resolution 1874 (2009),* S/2019/171, March 5, 2019, https://www.undocs.org/S/2019/171

[2] Ibid.

By September 2014, Kang Mun Kil had officially renamed Y Y Shun Limited as "Shunyi Limited", and this company provided a Chinese bank account for transfers from the Democratic People's Republic of Korea. The Member State informed the Panel that Kang Mun Kil's successor in China was Chong Won Ryol, a national of the Democratic People's Republic of Korea who is the official trade representative of the Democratic People's Republic of Korea in Dalian, China in addition to working on behalf of Namchongang Trading Corporation (a DPRK trading company subordinate to the General Bureau of Atomic Energy (GBAE) that was added to UN sanctions in 2009).

The pressure transducers ordered by North Korea had model numbers that included 140Z, 130Z, and 110Z. The companies' web pages, accessed in 2017, contained lists of its pressure transducers:

- CPCA-140Z: 1-1000 Torr
- CPCA-130Z: 0.1-100 Torr
- CPCA-110Z: 0.001-1 Torr

Pressure transducers covering these pressure ranges are similar to the ones sought by gas centrifuge plants. It should be noted that atmospheric pressure is 760 torr.

The reporting from a member state indicated that these pressure transducers were reverse-engineered from MKS designs. However, testing revealed that they were not as high-quality as the originals, having a failure rate in excess of ten percent. Evidently, they were of sufficient quality to have been purchased by North Korea for its uranium enrichment program. The North Korean purchase of the three types listed above was included in an order for computer controllers and subcomponents of frequency converters. The order, which was linked to the Yongbyon centrifuge plant, was made at a time that suggests this equipment was for the extension of the plant.

China's Non-Cooperation

The UN Panel requested information from China on these sales. In particular, it asked for information on "Shanghai Zhen Tai's sales of vacuum equipment and end users, correspondence between YY Shun Limited and Shanghai Zhen Tai and catalogues of the company's pressure transducers, relevant customs documents, immigration and visa record entries and exit information, and financial information."[3] China's response to the Panel, based on the information it had collected, was tepid and evasive. The Chinese government stated, according to the Panel report, "Shanghai Zhen Tai Instrument Corporation Limited does not have the export qualification in accordance with Chinese laws and regulations. Zhen Tai has neither directly carried out any export trade nor entrusted trade agent companies to do export on behalf of it since establishment," and, "regarding the Hong Kong company Y Y Shun

[3] Ibid.

Company Ltd and Shunyi Limited, after an in-depth investigation by China there is no evidence proving that they are operating in China on behalf of Namchongang Trading Corporation." China also told the Panel, "The bank account opened by the above Hong Kong companies in a Chinese bank has been closed," and "Kang Mun Kil left China in 2016 and is not in China now." The Chinese answers to the Panel of Experts contradict even the statements of Shanghai Zheng Tai on its own website, let alone those from the member state that provided the information documenting the orders and transfers of pressure transducers.

One also must ask if China is protecting Shanghai ZhengTai because it stole technology from MKS to develop its pressure transducers. According to one expert who reviewed the evidence and ZhengTai's equipment, they are "pretty good" copies of MKS pressure transducers. Although MKS does not have a patent on pressure transducers, there are many trade secrets involved in manufacturing them, that traditionally have allowed MKS to produce the world's top pressure transducers. However, their quality would indicate that if they are copies, they are not nearly as good.

Shanghai ZhengTai is still believed to be active, or at least its small factory that makes pressure transducers remains so. In recent years, it has sold its pressure transducers through over a dozen dealers in China, some of which change the labels on the equipment, a somewhat common practice among vacuum equipment sellers.[4]

This case also illustrates that there are many North Koreans in China that have good business relations with Chinese suppliers. The North Koreans, or their agents, focus on making sales appear to be domestic sales, which on the surface is not illegal. After buying the goods, the North Korean agents manage their transport to North Korea, which is usually illegal. Although the Chinese government is dissatisfied with North Korea's activities, and is doing more to disrupt them, its actions are still not effective enough. The Chinese export enforcement authorities are understaffed and have little help from domestic intelligence, a critical player in other countries in uncovering and preventing illicit trade. There is also a widespread attitude among Chinese government officials against undertaking any effort that goes against Chinese economic activities.

Case 4.2: Iran's Copying of Western Pressure Transducers[5]

In reaction to more stringent international controls, and despite the Iran nuclear deal, Iran has been bolstering its ability to build gas centrifuge-related equipment at the Fordow enrichment site during the last several years. This well-known site comprises both a deeply buried tunnel complex housing gas centrifuges, and an above-ground support area a few kilometers away

[4] See for example: http://www.ldxyq.com/products/show-5624712.html and http://www.rha51296004.com/products/show-5014872.html

[5] David Albright, Sarah Burkhard, Frank Pabian, and Jack Toole, "Conversion of Fordow: Another Unfulfilled Hope of the Iran Nuclear Deal," *Institute for Science and International Security,* July 10, 2019, http://isis-online.org/isis-reports/detail/conversion-of-fordow-another-unfulfilled-hope-of-the-iran-nuclear-deal

(see Figures 4.1 and 4.2). Iran recently announced the opening of key new centers at the support area, which in part aim to ease Iran's dependence on importing controlled goods for its centrifuge program through the establishment of what appear to be semi-indigenous nuclear-related equipment production lines to make pressure transducers.

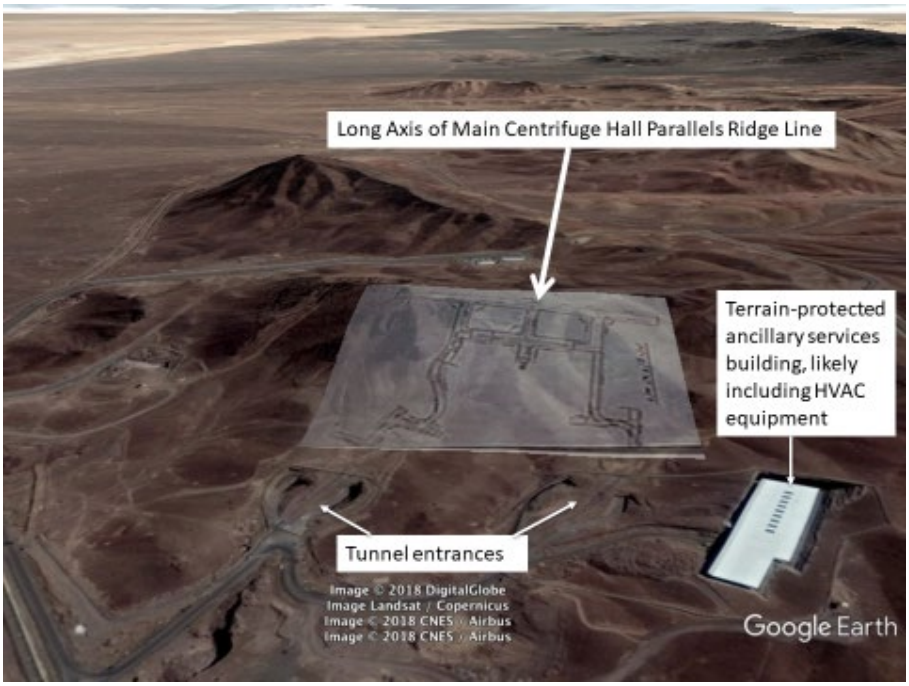


Figure 4.1. A 2018 Google Earth image with a schematic of the Fordow underground tunnel complex overlain. The schematic was found in the Iranian Nuclear Archive, seized by Israel from Tehran, as revealed by Israeli Prime Minister Benjamin Netanyahu on April 30, 2018.

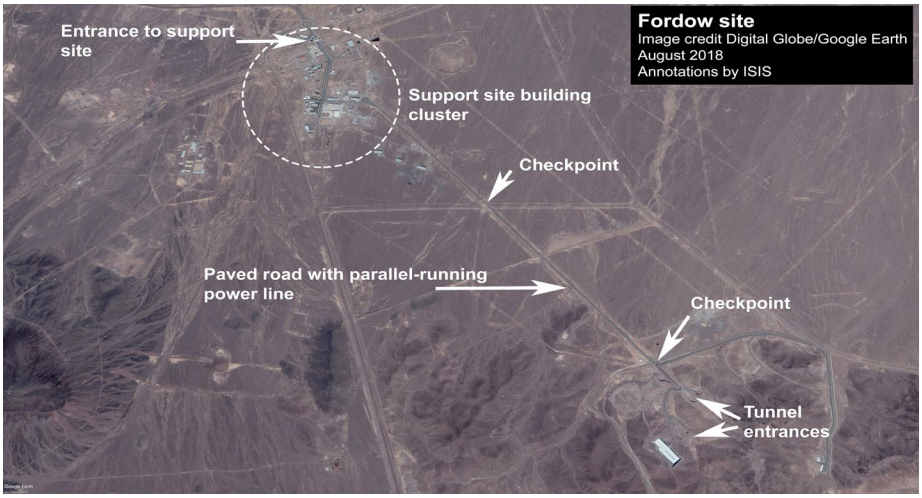


Figure 4.2. Overview of the Fordow facility, which includes the underground tunnel complex and the support complex. Given the relatively small size of the deeply buried tunnel complex, it would be too small to hold all the necessary ancillary operations of a gas centrifuge plant. Thus, an above-ground support area would be expected.

New Facilities at the Fordow Fuel Enrichment Plant

Two notable, recent construction projects in Iran are called the National Materials Science and Engineering Research Center and the National Vacuum Technology Center, introduced on Iran's National Nuclear Technology Day in 2018 and 2019, respectively. In promotional videos, Iran described the new research centers as a "scientific complex for industrial services of the nation."[6] That the facilities serve more than the gas centrifuge program is apparent. However, they also are critical to the gas centrifuge program, tied to its future and expected increase in capacity, and in particular, to its efforts to bypass international controls on sensitive goods needed in a gas centrifuge uranium enrichment program.

A 2019 promotional video distributed by the Atomic Energy Organization of Iran (AEOI) was used in conjunction with commercial satellite imagery to locate the vacuum center at the Fordow support area.[7] Figure 4.3, a Digital Globe image dated March 4, 2019, allows the correlation of the Vacuum Technology Center with footage from the promotional video taken at the facility. As can be seen, this center is near the central traffic circle at the site. Figure 4.4 shows its recent construction progress.

Using similar methods, including another promotional video, Figure 4.5 establishes the location of the National Materials Science and Engineering Research Center at the Fordow facility, which was inaugurated in April 2018. Based on the ground footage in this video, the authors were able to identify the building in overhead imagery.[8] According to a scientist interviewed in a media report accompanied by yet another video, this lab is the "first lab in the country being able to conduct tests on samples that are contaminated with radioactive radiation."[9] Further, the report listed ten different labs hosted in the research center: Sample Preparations, Metallography, Morphology Lab, Chemical Analysis, Mechanical Properties, Corrosion and Surface Engineering, Welding and Welding/Boiling Tests, Heat Treatment and Casting, Composite and Polymer Lab, and Ceramic Lab. Some of these capabilities are directly relevant to the vacuum center's efforts.

---

[6] "Iran Fordow National Materials Science and Engineering Research Center, New Laboratories," https://www.youtube.com/watch?v=MO9H6Dmepsw; Iran Atomic Energy Organization, "National Center for Vacuum Technology of Iran," https://www.aparat.com/v/N6Kc9 via automated Google Chrome translation of the title. Text in the video is in Farsi but was translated by a professional translator who consults with the Institute.

[7] Iran Atomic Energy Organization, "National Center for Vacuum Technology of Iran," https://www.aparat.com/v/N6Kc9. In Farsi but translated by Institute consultant.

[8] https://www.youtube.com/watch?v=MO9H6Dmepsw

[9] http://www.iribnews.ir/fa/news/2098301/%D8%A7%D9%81%D8%AA%D8%AA%D8%A7%D8%AD-%D9%85%D8%B1%DA%A9%D8%B2-%D8%AA%D8%AD%D9%82%DB%8C%D9%82%D8%A7%D8%AA-%D9%85%D9%87%D9%86%D8%AF%D8%B3%DB%8C-%D9%85%D9%88%D8%A7%D8%AF-%D8%B3%D8%A7%DB%8C%D8%AA-%D9%81%D8%B1%D8%AF%D9%88; https://www.mehrnews.com/news/4267121/%D9%85%D8%B1%DA%A9%D8%B2-%D8%AA%D8%AD%D9%82%DB%8C%D9%82-%D9%88-%D8%AA%D9%88%D8%B3%D8%B9%D9%87-%D8%B9%D9%84%D9%88%D9%85-%D9%85%D9%87%D9%86%D8%AF%D8%B3%DB%8C-%D9%85%D9%88%D8%A7%D8%AF-%D8%B3%D8%A7%DB%8C%D8%AA-%D9%87%D8%B3%D8%AA%D9%87-%D8%A7%DB%8C-%D9%81%D8%B1%D8%AF%D9%88-%D8%A7%D9%81%D8%AA%D8%AA%D8%A7%D8%AD. In Farsi but translated by Institute consultant.

Figure 4.3. Locating the Vacuum Technology Center at the Fordow facility. Image inset:
https://www.youtube.com/watch?v=MO9H6Dmepsw
http://shabestan.ir/detail/Photo/758447

Figure 4.4. Construction timeline of the Vacuum Center, clockwise from upper left.

Figure 4.5. Locating the National Materials Science and Engineering Research Center near the Vacuum Center. Image inset: https://www.youtube.com/watch?v=MO9H6Dmepsw http://shabestan.ir/detail/Photo/758447

National Vacuum Technology Center in more depth

On April 9, 2019, Iranian President Hassan Rouhani announced the opening and operation of the first phase of the Vacuum Technology Center, located at what the Iranians call the "Shahid Alimohammadi Enrichment Plant, Fordow."[10] Iran has used the name Shahid Masoud Alimohammadi to refer to the Fordow Fuel Enrichment Facility after Masoud Alimohammadi, a nuclear scientist with that name who was assassinated by a motorcycle bomb in 2010.[11] Alimohammadi is named in documents in the Nuclear Archive as a key member of Iran's former nuclear weapons program.[12] He was a member of the coordinating or planning staff of Project 3, another codename for Project 110, which was charged in the early 2000s with building five nuclear weapons and preparing an underground nuclear test site.[13]

Figure 4.6 is a freeze-frame of an Iranian video showing the main entrance of the Vacuum Technology Center. According to Qom's Governor Barham Sarmast, this center, constructed on 1,500 square meters of land in Qom, has an "important role in nuclear processes."[14]

The promotional video clip for the vacuum center features ground footage of the construction process and of the finished inside and outside of the building, as well as a statement by Ali Akbar Salehi, head of the AEOI of Iran. The voice-over narration explains the central purpose of the center to the AEOI and the applications of vacuum technology in the nuclear industry, and of a desire "to gather all the activities related to manufacturing, testing and calibration of vacuum equipment across Iran's atomic energy organization and to provide cross-organizational services and to create a domestic production line of capacitance pressure gauges."[15] According to the narrator, conducted research would also apply to the packaging and aerospace industry, among others. Dr. Salehi adds that the technology center is strategically located near the Materials Science and Engineering Research Center to facilitate collaboration.

Video footage from inside the center appears to show work on pressure transducers. Figures 4.7 and 4.8 are freeze frames of the video, in which persons appear to be making pressure

---

[10] http://www.iribnews.ir/fa/news/2396231/%D8%B1%D9%88%D9%86%D9%85%D8%A7%DB%8C%DB%8C-%D8%A7%D8%B2-%DB%B1%DB%B1%DB%B4-%D8%B7%D8%B1%D8%AD-%D9%88-%D8%AF%D8%B3%D8%AA%D8%A7%D9%88%D8%B1%D8%AF-%D9%87%D8%B3%D8%AA%D9%87%E2%80%8C%D8%A7%DB%8C. In Farsi but translated by Institute consultant.
[11] Saeed Kamali Dehghan, "Man Pleads Guilty to Assassinating Iranian Nuclear Scientist," *The Guardian,* August 23, 2011, https://www.theguardian.com/world/2011/aug/23/iran-nuclear-scientist-assassination-trial
[12] See for example, David Albright, Sarah Burkhard, Olli Heinonen, Frank Pabian, and Andrea Stricker, "Project Midan: Developing and Building an Underground Nuclear Test Site in Iran," *Institute for Science and International Security,* April 2, 2019, Annex 1, http://isis-online.org/isis-reports/detail/project-midan-developing-and-building-an-underground-nuclear-test-site-in-i/8
[13] Ibid.
[14] IRNA, "Iran Launches Vacuum Tech Center on Nuclear Day," April 9, 2019, https://en.irna.ir/news/83271635/
[15] Video in Farsi; translation by the Institute.

transducers. Figure 4.9, another freeze frame, appears to show a series of foreign-obtained pressure transducers connected to piping.

The National Vacuum Technology Center appears to have been built to reduce Iran's dependence on importing pressure transducers and other vacuum equipment needed for the uninterrupted operation and anticipated expansion of its gas centrifuge plants.

Iran has needed to illicitly import thousands of pressure transducers in order to operate its Fordow and Natanz enrichment plants. Many were made in the United States and subject to strategic trade controls as well as Iran sanctions.

As described in the introduction to this chapter, several actions, including improved sanctions, reformed internal corporate controls, and successful U.S. government prosecutions, such as of Chinese nationals involved in Iran's illicit commodity trafficking schemes, complicated Iran's overseas purchase of pressure transducers. These controls have even served as a form of a brake on Iran's enrichment program as it encountered difficulties in obtaining enough pressure transducers. The resulting scrutiny of Iran's procurements also provided a glimpse of the status and scope of Iran's centrifuge program, much of which has been secret.

Given that these transducers break frequently, and a steady supply is critical to the operation of gas centrifuge plants, it is unsurprising that Iran has sought to establish indigenous production capacities. It pursued a similar strategy with respect to vacuum valves needed for its gas centrifuge program (see Chapter C.3). However, despite its efforts to establish domestic transducer production, like in the case of vacuum valves, Iran will likely need to continue importing critical subcomponents of pressure transducers. Although the Iranian pressure transducer design is not known precisely, at least one of its subcomponents is likely controlled on suppliers' nuclear dual-use lists and would require a license for export to Iran. Based on prior Iranian procurement efforts, one such controlled subcomponent is made from Inconel, a special metal alloy, formed into a thin foil. Other difficult-to-make subcomponents that Iran is likely seeking to obtain from abroad for pressure transducers include vacuum feedthroughs and getters (see Chapter C.2).

Figure 4.6. Main entrance of the National Vacuum Technology Center as shown in a promotional video: https://www.aparat.com/v/N6Kc9

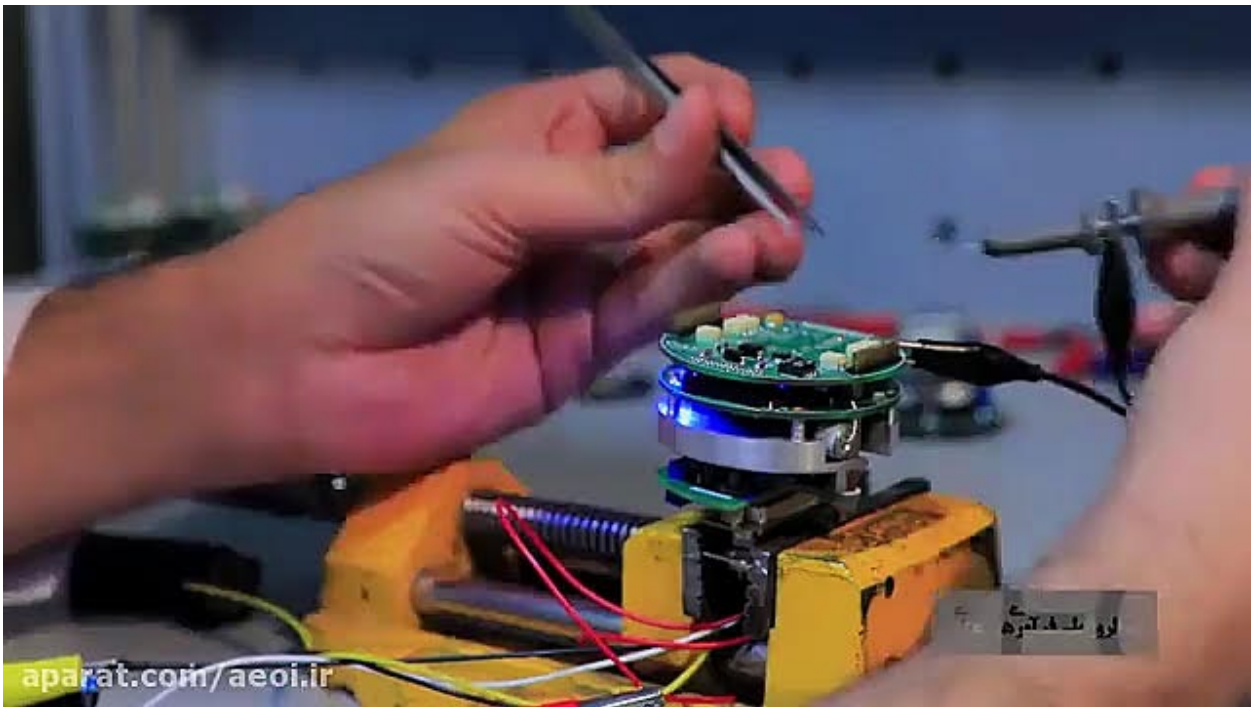


Figure 4.7. A freeze-frame from a promotional video published by the AEOI that appears to show a worker constructing a pressure transducer.

Figure 4.8. A worker enclosing a completed pressure transducer.

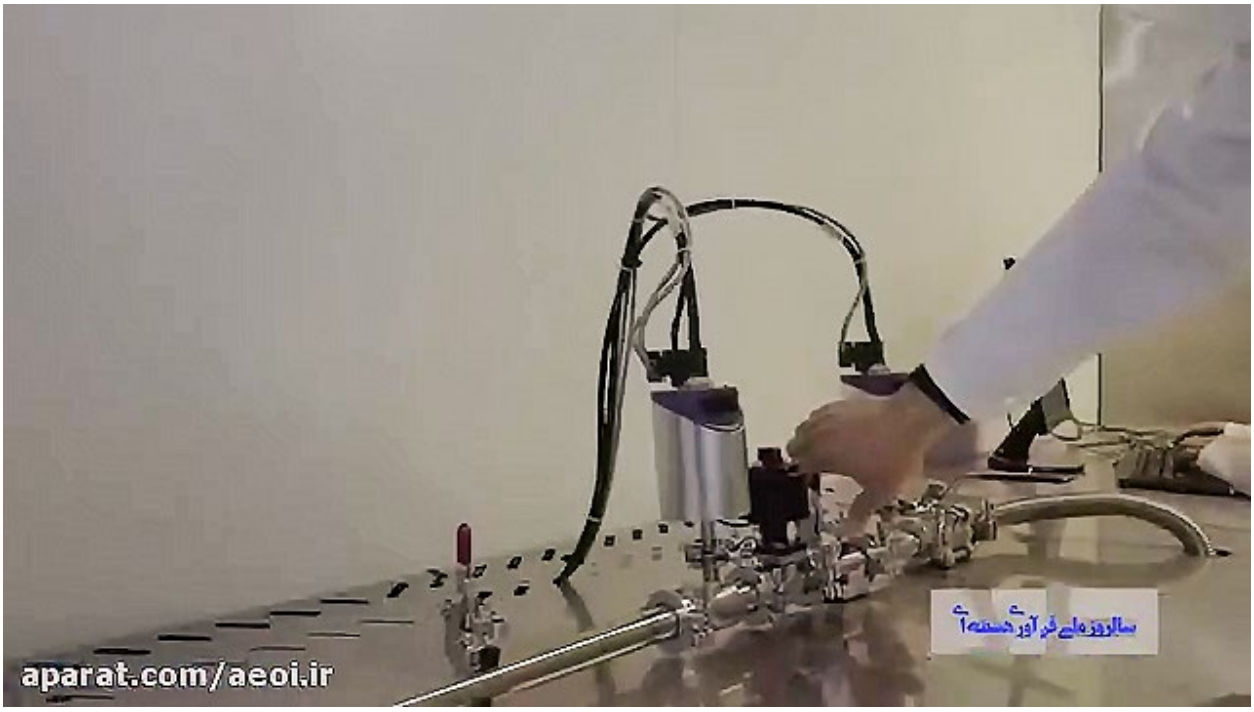


Figure 4.9. Another freeze-frame from the same AEOI video, showing what appear to be two pressure transducers connected to a thin pipe. The pressure transducers may have been obtained from abroad and not made in Iran.

Section II. Proliferation Financing

Chapter 5. Introduction to Proliferation Financing

Preventing proliferators of WMD and other destructive weapons from financing their illicit activities is an extremely difficult, but important effort. Paying for illicitly-acquired goods most often requires access to the international financial system, and the source of the funds for goods must be hidden from law-abiding financial institutions and national authorities. In other words, proliferant states and their illicit procurement networks must finance the purchase of strategic commodities by disguising the origin of financial transactions. This section first discusses the background of the growing number of efforts to counter proliferation financing, followed by several cases that describe various schemes that proliferators use to route bank transactions through often multiple countries before the funds finally reach the supplier and its bank account. This section also includes discussion of newer and more opaque, non-bank or virtual methods of financing proliferation.

The development of anything resembling a global regime of proliferation financing controls is in its infancy, as states and financial institutions struggle to implement and enforce basic controls and due diligence. Implementation by country and region also varies according to ability and interest.

It is ultimately in governments' and financial institutions' (as well as non-financial institutions') interest to implement strong counter-proliferation finance controls. Governments can build prosecutions and enact sanctions designations based on the uncovering of illicit finance schemes. Discovering proliferation finance schemes can often lead to the uncovering of entire illicit procurement networks. Financial institutions can avoid sanctions and penalties against them, as well as reputational hazards. Importantly, detecting and freezing such transactions can stymie proliferant states' import of needed goods used to augment their nuclear, WMD, missile, and military programs.

U.S. Leadership

The United States has underscored the importance of identifying and halting proliferation financing as a national priority, as evidenced by its inclusion in the 2017 *National Security Strategy (NSS)*. The NSS stated that the United States will prioritize the severing of sources of funding for proliferation activities: "We will deny revenue to terrorists, WMD proliferators, and other illicit actors in order to constrain their ability to use and move funds to support hostile acts and operations."[1] The U.S. *National Intelligence Strategy for 2019* also noted the need for the intelligence community to "implement a whole-of-government approach to advancing the enduring U.S. counterproliferation policy goals of discouraging interest in WMD, denying or

[1] *National Security Strategy of the United States of America,* December 2017, p. 34, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

disrupting acquisition, degrading programs and capabilities, including financial networks that fund proliferation activities, deterring use, and mitigating consequences."[2]

In fact, the United States has a unique opportunity to lead the global goal of attaining broader establishment of proliferation and other illicit finance counter-measures due to its preeminent power role and ability and willingness to use its economy as a means to pressure states into halting illicit activities and undertaking reforms. The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC), for example, are considered global standard-setters for financial controls and enforcement.[3] Many dollar-denominated transactions pass through U.S., and mainly New York-based, financial institutions since the dollar is the primary global reserve currency. Therefore, it is common for proliferant states and their networks to violate U.S. financial laws in the course of doing business, allowing it special leverage over detecting, preventing, and prosecuting proliferation financing as it occurs transnationally.[4]

The national, and broadly shared international, goal of preventing proliferation financing is not easily pursued due to the opaque nature and millions of financial transactions carried out each day. Schemes to route money from the actual end-user of an illicitly procured good to its supplier and intermediaries can be complex, involving more than one bank or financial entity and multiple transfers across borders. To defeat counter-proliferation financial controls, illicit procurement networks typically conceal the origin of a payment from financial institutions and the supplier and its government. They often use front companies and intermediaries located in third-party countries to carry out the transactions. For example, a transfer may start at a sanctioned country's bank and go to a second country's bank that does not levy sanctions against it, and then from that bank to the bank account of the supplier whose government has sanctions against the original state. Additional transfers can occur in-between that further obscure the origin. Money service businesses (MSBs) such as convertible virtual currency (CVC) exchanges are increasingly exploited by proliferant state schemes, and a lack of regulation in many of these newer, digital areas facilitates illegal activity.

It is difficult for even the most responsible of financial institutions to detect the illicit nature of transactions, even though they often employ extensive compliance departments and trained personnel, as well as advanced software and data analytics designed to detect money laundering and other illicit finance that would run afoul of domestic laws and sanctioned entity lists. In transaction paperwork or electronic entries, any description of the reason for a payment can be falsified (if one is even required), as well as information about individuals or entities making a payment. A financial institution can also never be certain of the accuracy of information about a claimed end-user of a proliferation-sensitive good. In countries where

---

[2] *National Intelligence Strategy of the United States of America for 2019,* p. 13, https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

[3] OFAC regularly shares guidance and tips with foreign authorities and financial institutions and discusses significant cases of concern by phone and other forms of communication.

[4] U.S. Department of Treasury, *National Proliferation Financing Risk Assessment for 2018,* https://home.treasury.gov/system/files/136/2018npfra_12_18.pdf

reporting of larger transactions is required, transactions can be split in order to fall below the reportable transaction thresholds, thereby reducing chances for detection. Some financial institutions are also complicit in furthering such schemes or turn a blind eye to the activity.

A modern phenomenon in proliferation financing, and one of the most difficult to counter, is a government's fund-raising efforts for proliferation-related activities. While a state's revenue and its access to assets overseas can be cut by imposing targeted financial and sectoral sanctions, these sanctioned governments can misuse alternative income sources and re-appropriate funds previously dedicated to legitimate projects (often at the expense of the well-being of the general public). Countries like Iran and North Korea use benign trade to raise money for proliferation-related activities, and instruct agents living in foreign countries to access and move funds back home. They may even exploit humanitarian good-exempt financial channels. Until these revenue streams or trading activities are identified as proliferation-related and appropriately sanctioned, such schemes are difficult to detect and prevent, since the visible transactions so often appear legal.

North Korea is one proliferator that uses bulk cash smuggling to finance illicit purchases, most often with witting partners, since cash can be moved without accessing the international financial system. Paying for goods using hard cash, rather than electronically, makes detection nearly impossible. But purchases made by proliferant states from legitimate, unwitting suppliers are different; these suppliers expect to conduct business, including being paid, in a normal manner, most often using electronic wire transfers, including via telegraphic transfers (T/T) or the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system, or letters of credit, which is a letter issued by a bank to another bank (especially one in a different country) to serve as a guarantee for payments made to an exporter under specified conditions. Front companies and intermediaries involved, whether witting or unwitting, also expect a profit for their efforts.

A newer method of financing illicit purchases is the use of digital assets or CVCs (cryptocurrencies), such as Bitcoin. FinCEN explains that "CVC is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of 'value that substitutes for currency.'"[5] According to the Foundation for Defense of Democracies, with regard to Bitcoin, "The Bitcoin software code enables users to send non-copyable digital assets, known as cryptocurrency or digital currency, to another person without an intermediary, removing the role of the traditional banking sector. The transaction history is stored on an immutable, distributed ledger known as a blockchain, with software code that typically is openly sourced and free."[6] Currently, it appears that most of these exchanges do not involve any identifiable personal information in transactions, favoring secrecy. These digital

[5] U.S. Department of Treasury, Financial Crimes Enforcement Network (FinCEN), "FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Currencies," May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[6] Key threats by state actors using blockchain and cryptocurrency are discussed further in: Yaya J. Fanusie and Trevor Logan, "Crypto Rogues: U.S. State Adversaries Seeking Blockchain Sanctions Resistance," *Foundation for Defense of Democracies,* July 11, 2019, https://www.fdd.org/analysis/2019/07/11/crypto-rogues/

exchanges risk facilitating illicit payments and removing opportunities for detection altogether. Bitcoin states on its website that, like any other currency, it could be used "for both legal and illegal purposes." It states, "Attempting to assign special rights to a local authority in the rules of the global Bitcoin network is not a practical possibility…It is however possible to regulate the use of Bitcoin in a similar way to any other instrument."[7] One challenge for authorities could be locating and regulating entities which lack anything resembling an administrative or operational center of activities. Some blockchain analysis firms, however, claim they have "engaged directly with global regulators."[8] In May 2019, U.S. authorities issued new, strong guidance directed at individuals, financial institutions, and money service businesses to warn and help them avoid making or facilitating illegal transfers via CVCs.[9] The guidance made clear that violators will be held accountable.

A new global challenge is state-directed cyber-attacks aimed at outright theft of money from financial institutions and other entities. Around 2013, North Korea began deploying cyber-attack groups, namely its APT38 and Lazarus Group, to carry out egregious, lucrative thefts from banks and cryptocurrency exchanges, which enabled it to more easily generate revenue than it otherwise could via complex financial transfer schemes. In 2019, according to the August 2019 UN Panel of Experts report on North Korea, North Korea carried out cyber-attacks against 35 entities in 17 countries and stole or attempted to steal around $2 billion from "financial institutions, cryptocurrency exchanges and mining activity designed to earn foreign currency," which it could then use to finance its WMD programs.[10] In addition, North Korea, and most recently, Iran, have pursued currency counterfeiting schemes by printing large amounts of counterfeit foreign banknotes to facilitate proliferation and other purchasing schemes.[11] Proliferant states have also used precious metals to finance purchases. They may involve their central banks, universities, domestic shipping assets, and airlines to physically move money or commodities used as currency and front illicit electronic transfers, to name a few methods.

---

[7] Bitcoin, "Frequently Asked Questions," https://bitcoin.org/en/faq#general

[8] Hisashi Oki, "What to Expect at G-20: Money Laundering and Crypto Discussion," *CoinTelegraph,* June 9, 2019, https://cointelegraph.com/news/what-to-expect-at-g-20-money-laundering-and-crypto-discussion

[9] FinCEN, "FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Currencies."

[10] *Report of the United Nations Panel of Experts established pursuant to Resolution 1874 (2009),* S/2019/691, August 30, 2019. Annex 21 contains a list of suspected North Korean cyber attacks on banks and cryptocurrency exchanges reported to the Panel since 2015.

[11] According to a German domestic intelligence report, for example, on March 1, 2018, an Iranian national was sentenced to seven years in prison for currency counterfeiting and violating European Union sanctions against Iran. According to the report, Iran would have been able to print large amounts of money with the help of the convicted individual and his Germany-based company. The investigation discovered that the company produced about 50 million counterfeit Yemeni banknotes. The intelligence report is an annual publication by the Federal Office for the Protection of the Constitution. It was published in June 2019 and covers the year 2018. See: German Federal Office for the Protection of the Constitution, "Verfassungsschutzbericht 2018," June 2019, Available in German at: https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte/vsbericht-2018

Role of Financial Institutions

According to an estimate by the Bank for International Settlements, around one-third of global trade transactions involve "bank-intermediate trade finance," with a high share of trade financing occurring in the Asia-Pacific.[12] When a bank is involved as an intermediary, some documentation is required, which can provide banks with information that can be used in screening for bad actors or illicit activity. In trade transactions occurring as open account practice, payment is due after the delivery of goods, but other transactions take place on pre-pay terms, or before the goods are shipped. A typical cash-in-advance arrangement is a supplier receiving a deposit of 30 percent of the goods' value before their production and a final payment of 70 percent before shipment. Payments most commonly made in the form of international wire transfers provide the minimal basis for banks to apply screening methods. Other traditional methods of payment for trade include, as described, letters of credit, but also credit cards (with additional obstacles for use transnationally), escrow service (where funds are held in custody until the transfer of goods is made and quality is assured), or payment by check (which may entail lengthy wait periods for non-domestic checks).[13]

Countries that carefully enforce UN sanctions and domestic laws against transactions with countries of proliferation concern require banks to bear a large onus in preventing proliferation financing. They are required to comply with domestic financial laws and conduct "due diligence" to determine the nature of their customers and transactions. Banks may be required to report transactions over a certain amount, not process transactions and freeze those associated with sanctioned countries, entities, or individuals, and report and disclose transactions attempted or made successfully by such parties. The United States requires its financial institutions to submit Suspicious Activity Reports (SARs) for potentially criminal transactions and report on cash transactions exceeding $10,000.[14] Because illicit networks can conceal names of individuals and entities, and rarely list controlled goods as part of a financial transaction, it is particularly difficult for banks to detect proliferation financing schemes, unless they are made directly from a sanctioned financial institution or by individuals on sanctions lists. Often only repeat, suspicious transactions or red flag indications of involvement of banned parties, entities, or countries will tip off financial institution compliance personnel or screening software to the possibility of illicit behavior. An anonymous sanctions compliance specialist at a Southeast Asian bank, who regularly faces risks of accidentally facilitating North Korean business, told *NK News*, "We have to prove beyond doubt that a certain institution that

[12] Bank for International Settlement: Committee on the Global Financial System, "Trade Finance: Developments and Issues," CGFS Papers, No. 50, January 2014, https://www.bis.org/publ/cgfs50.pdf

[13] David Noah, "Methods of Payment in Advance in International Trade: Cash in Advance," Shipping Solutions, *International Trade Blog*, July 22, 2019, https://www.shippingsolutions.com/blog/methods-of-payment-in-international-trade-cash-in-advance?utm_campaign=International%20Trade%20Blog&utm_source=hs_email&utm_medium=email&utm_content=74899897&_hsenc=p2ANqtz--4sIsjCrHmzjM00ozuKeTGtgmJVc-gX5g-3JpAPBXI19_SCFkNBYcbCGweDmgd9mzWhaUrc-Y1Gg-ydUv-DOxKZu97pw&_hsmi=74987041

[14] Office of the Comptroller of the Currency, "Suspicious Activity Reports (SAR)," https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html

[is] probably near some sanctions exposure does not cause a sanctions exposure to come near to our bank… regulators have left it to the banks to de-risk."[15]

De-risking for financial institutions includes heavy reliance on sanctioned entity lists, as described, but also on "ring-fencing." This means that bank accounts or transactions that are banned or have been frozen can lead to other candidate entities and banks involved in or at-risk for illicit involvement, and absent complete proof of illicit activity, they are "ring-fenced" and stopped from making transactions.[16] Financial institutions also investigate their customers' profiles and activities in order to assess risk, including such features as their foreign national status, country of origin, nature of business, and financial habits. For example, the opening of multiple accounts and operating many trading companies or similar businesses might constitute adequate risk for a financial institution to deny a customer the ability to use its services. A similar approach is taken with processing currency-clearing transactions, particularly those in dollars and Euros. The difficulty of the compliance task is underscored by the compliance specialist at the Southeast Asian bank, who stated, "Trading is all trading on documents…And that's where the problem lies. If you are trading on paper, you have to trust the paper. How many resources do I have to put behind a piece of paper?... How do we ring-fence the risk of such illicit trades?...The banks lack this information."[17]

To assist their efforts, financial institutions often cooperate closely with their regulating authorities in countries with strong regulations, and even foreign authorities such as OFAC, in order to minimize risk. However, financial institutions do not always receive detailed feedback from regulators about their reports and any underlying schemes. They also look to larger, peer banks that are considered standard-setters, and to their correspondent banks in foreign countries, as models for action and collaborators in threat and risk information sharing. Regarding general threat information gathering, financial institutions are increasingly relying on threat intelligence centers, whether independent from the institution or developed internally.[18] With specific transactions and customers, however, they may be prevented from sharing information transnationally due to privacy and confidentiality laws. In general, in the United States and elsewhere, the ability of financial institutions is quite limited to liaise with enforcement authorities, customs agencies, sensitive commodity suppliers, and shippers, who might add to their understanding of specific transactions or proliferation financing schemes more broadly.

While responsible financial institutions in strongly-regulated countries look hard to detect anything suspicious in transactions or about their customers and investigate them, major financial institutions have been complicit in allowing proliferation financing schemes to go on, resulting in massive fines, for example, by the United States and Europe. The United States has

[15] Chad O'Carroll, "An Insider's View: How Banks Try to Avoid North Korea Sanctions Risks," *NK News,* July 11, 2019, https://www.nknews.org/2019/07/an-insiders-view-how-banks-try-to-avoid-north-korea-sanctions-risks/?c=1562845144318

[16] Ibid.

[17] Ibid.

[18] Ibid.

demonstrated little tolerance for the witting, illegal processing of dollar-denominated transactions or dollar-clearing efforts on behalf of sanctioned countries or entities.[19] It sanctions rogue banks that routinely cooperate with banned parties and countries.

Counter-Proliferation Finance Measures and the Global State of Controls

Several international, regional, and national efforts attempt to improve the chances of detecting and preventing the growing exploitation of financial avenues by proliferation networks. In 2004, the international community passed UN Security Council Resolution 1540, which recognized the need for all nations to put in place appropriate, effective trade and financial controls to prevent the illicit procurement and financing of WMD-related equipment and materials.[20]

Several UN resolutions passed in support of Resolution 1540 have highlighted the need for states to work toward better implementation of counter-proliferation finance controls, in particular UNSCR 2325 (2016), which noted a "need for more attention on…proliferation finance measures…"[21] The UNSC has also passed resolutions relating to the prevention of Iran's and North Korea's illicit financing for their sanctioned nuclear, missile, and military programs, namely UNSCR 2231 (2015) on Iran (which replaced earlier resolutions terminated under the 2015 nuclear deal, the Joint Comprehensive Plan of Action or JCPOA), and UNSCR 1718 (2006) and successor resolutions on North Korea, such as UNSCRs 2087 (2013) and 2321 (2016). These resolutions mandated the designation and freezing of assets of key individuals, entities, or sectors identified as engaged in proliferation financing. As such, the actions of states and financial institutions to implement both broad counter-proliferation finance measures and those pertaining to specifically sanctioned states, entities, and individuals, rest on a sound international legal foundation.

The Financial Action Task Force (FATF), a Paris-based inter-governmental organization, supports stronger global counter-proliferation financing efforts and relevant UN resolutions by facilitating the development and implementation of globally-recognized standards for countering proliferation finance, money laundering, terrorist financing, and other financial

---

[19] In 2019, a fine of $1.1 billion was levied by OFAC and various U.S. agencies against Standard Chartered Bank of London for repeatedly carrying out banned transactions with Iranian, Cuban, Syrian, Burmese, and Sudanese entities. See: Karen Freifeld, "Standard Chartered to Pay $1.1 Billion for Sanctions Violations," Reuters. April 9, 2019, https://www.reuters.com/article/us-stanchart-sanctions-settlement-fed/standard-chartered-to-pay-1-1-billion-for-sanctions-violations-idUSKCN1RL1TV#targetText=The%20agreement%20has%20been%20extended,also%20included%20the%20FCA%20penalty. The United States has also imposed multi-million-dollar fines against a number of other foreign banks, such as BNP Paribas (a massive $8.9 billion in 2014), France's Credit Agricole ($787 million in 2015), ING Bank in Amsterdam ($619 million in 2012).

[20] United Nations Security Council, *Resolution 1540 (2004),* April 28, 2004, https://undocs.org/S/RES/1540(2004)

[21] See: UN Resolution 1540 Committee, "Security Council Resolutions," https://www.un.org/en/sc/1540/resolutions-committee-reports-and-SC-briefings/security-council-resolutions.shtml ; UNSC, *Resolution 2325 (2016),* https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2325.pdf

crimes by countries and their financial institutions.[22] These international standards are described in the "40 FATF Recommendations."[23] FATF and FATF-style regional bodies whose membership is governments carry out "mutual evaluations," which involves in-country reviews to assess how states are performing individually at implementing FATF recommendations. Examples of recommendations relevant to countering proliferation financing are those that address a jurisdiction's ability to implement targeted financial sanctions based on UNSCRs, basic measures such as interagency cooperation and coordination, and supervision and monitoring of financial institution compliance.[24] FATF tracks implementation of requirements by countries to freeze the "funds, other financial assets and economic resources" of UNSCR-designated entities or those controlled by them. Its standards also comprise steps to safeguard against illicit transactions that involve proliferation, but fall outside UN resolutions. To supplement the recommendations, FATF issued and has continued to update a separate report providing guidance for preventing the financing of proliferation and for the implementation of financial measures of UNSCRs.[25] Resolution 1540's implementing resolutions support and recognize the work of the FATF.

Most countries still do not have strong legal measures in place to detect and prevent proliferation financing, a finding supported by FATF mutual evaluations. For mutual evaluation data on 75 countries and territories that were surveyed by FATF in its fourth round of ratings as of April 2019,[26] a significant portion of countries have poor effectiveness with regard to proliferation financing.[27] Under FATF Recommendation 7, which stipulates that countries should enact and enforce "targeted financial sanctions related to proliferation," 47 countries were only partially compliant or completely non-compliant. For FATF Immediate Outcome 1, "Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation," only one country had high effectiveness, while 50 countries had either medium or low effectiveness. Perhaps most relevant to preventing proliferation financing, under FATF Immediate Outcome 11, "Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs," only two countries had high effectiveness, while 57 countries had either medium or low effectiveness.

---

[22] FATF, "Who We Are," http://www.fatf-gafi.org/about/

[23] FATF, "The FATF Recommendations," updated October 2018, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

[24] FATF, *FATF Guidance on Counter Proliferation Financing: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction,* February 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf The FATF Guidance includes detailed descriptions of UNSCR and other general counter-proliferation finance standards for which it seeks to promote effective implementation.

[25] *FATF Guidance on Counter Proliferation Financing*.

[26] The fourth round of rating started in 2014 and was on-going at the time of this writing.

[27] FATF, "Fourth Round Ratings," table updated April 17, 2019, https://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf

The FATF's findings about poor proliferation financing controls are supported by the findings of the Institute for Science and International Security's own *Peddling Peril Index (PPI) for 2019/2020,* which assesses the performance and strength of national strategic trade controls in 200 countries, territories, and entities. The PPI found that only eleven countries achieved more than half of the available points in the index under the criterion *Ability to Prevent Proliferation Financing*.[28] This means that more than 90 percent of countries largely underperform at preventing proliferation financing. Forty-one countries surveyed had negative scores because they lacked basic financial controls or contributed to proliferation and other illicit finance. PPI data supports that the United States is one of the top performers in countering proliferation financing, as a leader in regulatory efforts, enforcement, and private sector outreach aspects.

Other major concerns pertaining to states' effectiveness in preventing and detecting proliferation finance include a lack of relevant domestic legislation in place directing financial institutions to enforce UN and domestic sanctions, lack of timeliness in states adding to entity lists and then informing financial institutions, and delays in financial institutions acting on state decisions and information. In addition, poor effectiveness of risk management efforts by financial institutions remains a significant problem.[29]

The FATF has taken note of the growing threat of misuse of virtual currencies to contribute to proliferation financing. In June 2019, with the support of the G20 group of countries and UN Resolution 2462 (2019), it adopted an Interpretive Note to Recommendation 15 on New Technologies (INR. 15) aimed at "prevent[ing] the misuse of virtual assets for money laundering and terrorist financing and the financing of proliferation." FATF stated:

> *The obligations require countries to assess and mitigate their risks associated with virtual asset activities and service providers; license or register service providers and subject them to supervision or monitoring by competent national authorities—(notably, countries will not be permitted to rely on a self-regulatory body for supervision or monitoring)—and implement sanctions and other enforcement measures when service providers fail to comply with their AML/CFT [anti-money laundering/counter-terrorist financing] obligations; and underscore the importance of international cooperation. Some countries may decide to prohibit virtual asset activities based on their own assessment of the risks and regulatory context, or to support other policy goals.*
>
> *Further, INR. 15 requires countries to ensure that service providers also assess and mitigate their money laundering and terrorist financing risks and implement the full range of AML/CFT preventive measures under the FATF Recommendations, including*

[28] David Albright, Sarah Burkhard, and Andrea Stricker, The *Peddling Peril Index for 2019/2020* (Washington, D.C.: Institute for Science and International Security, May 2019), http://isis-online.org/uploads/isis-reports/documents/The_Peddling_Peril_Index_Final_May2019.pdf

[29] Togzhan Kassenova, "Challenges with Implementing Proliferation Financing Controls: How Export Controls Can Help" (Washington, D.C.: Carnegie Endowment for International Peace, appearing also in *World ECR*, May 30, 2018), https://carnegieendowment.org/2018/05/30/challenges-with-implementing-proliferation-financing-controls-how-export-controls-can-help-pub-76476

> *customer due diligence, record-keeping, suspicious transaction reporting, and screening all transactions for compliance with targeted financial sanctions, among other measures, just like other entities subject to AML/CFT regulation.*[30]

If they have not already, member states will need to pass relevant legislation regulating the activities of financial institutions with regard to transactions with CVCs. FinCEN's May 2019 guidance, for example, stated that money service businesses must apply the "Funds Travel Rule" to CVC activities in U.S. jurisdictions, requiring them to collect identifying information on transactions with CVCs or on behalf of a customer transacting with a CVC, if the transfer is in the amount of $3,000 or more.[31] Such efforts strive to remove the cloak of secrecy created by CVC transactions and allow for better regulation.

Recognizing the growing threat of state-directed cyber-attacks and exploitation of virtual assets to fund proliferation activities, the UN Panel of Experts on North Korea recommended that countries:

> *…Ensure their regulations cover virtual currency and non-banking financial institutions and money services businesses, including cryptocurrency exchanges, and that they ensure that these exchanges share the same obligations assigned to banks to prevent the laundering of funds; this enhanced vigilance would apply to monitoring suspicious transactions, providing governments with information on accounts after attacks, freezing assets of sanctioned entities and blocking transactions from accounts controlled by malicious actors.*[32]

The FATF has recently gone beyond urging only financial institutions to be on alert over proliferation finance schemes in the context of sanctions evasion. In its 2018 *Guidance on Counter Proliferation Financing,* it recommended "extending monitoring to those sectors which do not fall under the definition of financial institution or DNFBPs [Designated Non-Financial Businesses or Professions] but are vulnerable to proliferation financing (e.g. maritime insurers or dual-use goods exporters)." For example, insurers could play a key role in stopping the insuring and underwriting of activities of maritime vessels and airplanes that would engage in sanctions-circumventing activities. In one study, the Royal United Services Institute (RUSI) closely investigated the role of insurers, re-insurers, and brokers in detecting and preventing proliferation finance. Several anonymous interviewees reported that insurance and brokering

---

[30] FATF, "Public Statement on Virtual Assets and Related Providers," June 21, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html

[31] FinCEN, "FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Currencies."

[32] "38North Interview with Stephanie Kleine-Ahlbrandt on the UN Panel of Experts Latest Report to the Security Council Published Today," *38North,* September 5, 2019, https://www.38north.org/2019/09/skleineahlbrandt090519/?utm_source=Stimson+Center&utm_campaign=2e98d28c83-38NDigest%2FEast+Asia%2F38+North+Digest_0901&utm_medium=email&utm_term=0_15c3e20f70-2e98d28c83-46296593&mc_cid=2e98d28c83&mc_eid=76a39e2d5e

communities currently consider proliferation finance little or not at all.[33] FATF, in its guidance, encouraged such "non-financial institutions to leverage on existing risk-based measures to identify potential customers and transactions that could be involved in sanctions evasions."[34]

Countering Iran's Proliferation Financing

Iran has received special attention because of the sheer volume of U.S. and international sanctions applied against Tehran. Iran's proliferation financing activities are often part of its larger strategic trade control and sanctions-busting efforts which seek to circumvent global or national controls on its ability to fund its military, ballistic missile, nuclear, and other WMD programs. The UN Security Council previously sanctioned dozens of Iranian entities and individuals for their involvement in nuclear, missile, and military activities. Following the implementation of the JCPOA in early 2016, the UN Security Council moved to lift sanctions on many of these parties under the accord's implementing resolution, UNSCR 2231 (2015). However, it put in place a nuclear procurement channel that requires UNSC notification and approval given by a JCPOA member state "Procurement Working Group" in order for Iran to import nuclear direct and dual-use goods. Absent UNSC authorization, UNSCR 2231 maintains embargoes on Iran's import of ballistic missiles and related goods, and cruise missile and conventional military-related goods, which are slated to lift in October 2020 and October 2023, respectively.[35] Therefore, Iran's illicit financing of nuclear, missile, and military procurements remain prohibited and UN member states must take steps to prevent this activity.

In 2008, FATF began to list Iran in its annual public statements as a country with anti-money laundering and counter-financing terrorism deficiencies so severe that countermeasures should be applied by financial institutions around the globe. The only other country for which FATF had called for such drastic measures was North Korea. Iran remained on the list of "high-risk and non-cooperative jurisdictions" for seven subsequent years, until, in June 2016, Iran submitted an Action Plan and agreed to cooperate with the FATF to undertake reforms. While Iran was still called a "high-risk jurisdiction," the call for countermeasures was suspended. However, the Action Plan expired in January 2018 with only one out of ten items completed.[36] Since then, at its triannual meetings, which occur every February, June, and October, FATF has deferred the question of urging countries to re-impose all countermeasures.[37] During that time, Iran fulfilled two additional items on its Action Plan. In June 2019, the FATF followed through on a February 2019 warning that it would "require increased supervisory examination for branches and subsidiaries of financial institutions based in Iran," should Iran not have its

[33] Emil Dall and Tom Keatinge, "Underwriting Proliferation Financing: Sanctions Evasion, Proliferation Finance and the Insurance Industry" (London: Royal United Services Institute, RUSI Occasional Paper, July 2018), p. 6, https://rusi.org/sites/default/files/20180710_underwriting_proliferation_web.pdf
[34] *FATF Guidance on Counter Proliferation Financing*, February 2018, p. 14.
[35] United Nations Security Council, *Resolution 2231 (2015),* http://unscr.com/en/resolutions/doc/2231
[36] FATF, "Public Statement - October 2018," Paris, France, October 19, 2018, https://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-october-2018.html
[37] See a series of FATF Public Statements, dated February 23, 2018, June 29, 2018, October 19, 2018, February 22, 2019, June 21, 2019, and October 18, 2019: http://www.fatf-gafi.org/countries/#Iran

Action Plan fulfilled.[38] FATF announced that Iran would face additional countermeasures should it fail to "enact the Palermo and Terrorist Financing Conventions in line with the FATF standards," which is part of item six of the Action Plan, by October 2019. It gave Iran "a final deadline" to fulfill its demands by February 2020 before it would re-impose all countermeasures.[39] At the October 2019 meeting, FATF stated that it decided to:

> ***…****Call upon its members and urge all jurisdictions to introduce enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in Iran. If before February 2020, Iran does not enact the Palermo and Terrorist Financing Conventions in line with the FATF Standards, then the FATF will fully lift the suspension of counter-measures and call on its members and urge all jurisdictions to apply effective counter-measures, in line with [FATF's] recommendation 19.*[40]

Decisions by Iran's law-making parliament and councils, including the rejection of the Palermo bill the day before the October plenary meeting began, as well as debate among Iran's senior government officials, indicate that it is unlikely Iran will ever fulfill the Action Plan.[41]

The United States specifically blacklists numerous Iranian entities engaged in proliferation financing, WMD procurement, terrorist activities, and human rights abuses and maintains a general embargo on trading or financing activity with Iran. In mid-2018, following the U.S. exit from JCPOA, many Iranian entities that had been granted sanctions relief once again became subject to U.S. financial sanctions, such as the Central Bank of Iran (CBI).[42] These sanctions also threaten penalties against financial institutions that conduct business with a sanctioned Iranian entity or engage in dollarized transactions with Iran. In April 2019, the United States designated the Islamic Revolutionary Guards Corps (IRGC) as a foreign terrorist organization (FTO), which, along with economic penalties, carries criminal penalties for engaging in transactions with an IRGC-linked individual or entity.[43] In June 2019, the United States

---

[38] FATF, "Public Statement - June 2019,"Orlando, FL, United States, June 21, 2019, http://www.fatf-gafi.org/countries/d-i/iran/documents/public-statement-june-2019.html

[39] "Global Watchdog Gives Iran until Feb to Tighten Anti-Money Laundering Rules," Reuters. October 18, 2019, https://www.reuters.com/article/us-fatf-iran/global-watchdog-gives-iran-until-feb-to-tighten-anti-money-laundering-rules-idUSKBN1WX167

[40] FATF, "Public Statement – October 2019," Paris, France, October 18, 2019, http://www.fatf-gafi.org/countries/d-i/iran/documents/public-statement-october-2019.html

[41] "Palermo Bill Off Agenda: Expediency Council Member," *Mehr News Agency,* October 14, 2019, https://en.mehrnews.com/news/151223/Palermo-bill-off-agenda-Expediency-Council-member; Rohollah Faghihi, "Iranian Hard-liners Leverage IRGC Terrorist Designation to Kill FATF Bills," *Al-Monitor*, April 17, 2019, https://www.al-monitor.com/pulse/originals/2019/04/iran-irgc-fto-designation-fatf-bills-expediency-council.html

[42] See, for example, entities previously sanctioned for illicit financial and other malign activities: U.S. Department of Treasury, "Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism," October 25, 2007, https://www.treasury.gov/press-center/press-releases/pages/hp644.aspx

[43] Nicole Gaouette, "Trump Designates Elite Iranian Military Force as a Terrorist Organization," CNN, April 8, 2019, https://www.cnn.com/2019/04/08/politics/iran-us-irgc-designation/index.html

designated the Supreme Leader of Iran and blocked his, as well as associated persons' property, among other new sanctions.[44] In September 2019, the United States also placed additional terrorism-related sanctions on the CBI and National Development Fund.[45] Iran's U.S.-sanctioned entities have also been disconnected from making SWIFT transactions, SWIFT being a Belgian firm that processes global financial messages relating to wire transfers and transactions.[46]

The European Union, which retains sanctions relief with Iran, is attempting to set up a special mechanism for trade with Iran in sanctions-exempt goods in order to avoid transacting in dollars. This "special purpose vehicle (SPV)" is called INSTEX, or Instrument in Support of Trade Exchanges.[47] It is apparent, however, that the mechanism will not provide the meaningful economic relief promised to Iran under the JCPOA. Overall, U.S. actions are creating a chilling effect on international business with Iran, given the long reach of Iran's military establishment into a variety of major sectors and uncertainty on the parts of companies and banks about whether to take risks. As a result, Iran's black market and illicit financial activity is increasing.

Iran's financial system is entirely cut off from the U.S. financial system apart from channels for payments for humanitarian and agricultural products. But since the U.S. dollar is the world's major trading currency, Iran seeks ways to convert, launder, or move money using both U.S. and non-U.S. financial institutions. On the proliferation finance level, Iran typically routes payments from its proliferation programs and domestic contractors or trading companies via central banks, foreign trading companies' bank accounts, and increasingly, non-traditional means such as barter, exchange house, and ledger transfer schemes. The 2018 U.S. *National Proliferation Financing Risk Assessment* noted, however, that in contrast to North Korean proliferation financing schemes, "Iranian PF [proliferation financing] cases…have mainly focused on procurement" but with "notable recent exceptions."[48] The report stated that following the JCPOA's implementation, Iran may have had "less of a need to employ the same covert fundraising and fund movement practices globally that it previously did to support its weapons programs, and the regime more broadly."[49]

Iran has apparently not yet entered extensively into the business of carrying out cyber-attacks to steal funds from banks and other institutions, as North Korea has. Its efforts have mostly

---

[44] The White House, "Executive Order on Imposing Sanctions with Respect to Iran," June 24, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-imposing-sanctions-respect-iran/

[45] The CBI was originally sanctioned in 2012, sanctions were lifted as part of the JCPOA, and then re-instated. The terrorism sanctions enhance the previous designation. U.S. Department of Treasury, "Treasury Sanctions Iran's Central Bank and National Development Fund," Press Release, September 20, 2019, https://home.treasury.gov/news/press-releases/sm780

[46] Arshad Mohammed, "SWIFT Says Suspending Some Iranian Banks' Access to Messaging System," Reuters. November 5, 2018, https://www.reuters.com/article/us-usa-iran-sanctions-swift/swift-says-suspending-some-iranian-banks-access-to-messaging-system-idUSKCN1NA1PN

[47] Leila Gharagozlou, "EU Implements New Iran Trade Mechanism," CNBC, January 31, 2019, https://www.cnbc.com/2019/01/31/eu-implements-new-iran-trade-mechanism.html

[48] *National Proliferation Financing Risk Assessment for 2018,* p. 19.

[49] Ibid.

been to wreak havoc in retaliation for policy or security actions by the United States. In one instance, from 2011 to 2012, Iranian government-backed hackers carried out a "distributed denial of service" cyber-attack against 46 U.S. banks. Customers were unable to access their funds, but the main practical result of the attack was the vast cost to the targeted financial institutions to remediate it. In March 2016, the Department of Justice indicted seven alleged Iranian conspirators behind that cyber-attack.[50]

Countering North Korean Proliferation Financing

The international community has decided in several United Nations resolutions to prevent the illicit financing activities of North Korea that support its proliferation programs. As in the case of Iran, the United States has applied extensive additional unilateral sanctions on North Korea.

Illicit procurement funded by the North Korean state and other revenue-raising schemes have been traced to North Korea's sale of certain commodities, as well as other trade and non-financial activities, resulting in targeted UN sanctions to curtail it. Financial measures encoded in several UN resolutions include actions that countries must undertake with regard to North Korean activity on their territories, such as: preventing the provision of financial services, including bulk cash and gold, grants, financial support, or loans that could assist sanctions evasion; prohibition against allowing the opening of North Korean bank branches, closure of existing ones, termination of joint business ventures, ownership interests, and correspondent banking relationships and disclosure of existing relationships; prohibition against opening of bank accounts in North Korea; prohibition of trade support such as export credits, insurance, or guarantees; if an individual is determined to be working on behalf of a North Korean financial institution, they must be expelled from the state; and asset freezes for those entities and individuals that support North Korean illicit or sanctioned activities, including maritime vessels. A complete list of measures is available on the UN Security Council Resolution 1787 (2006) website.[51]

Together, if implemented, these measures are intended to stop or slow North Korea's import of proliferation-sensitive commodities by preventing their financing, as well as stem the fundraising for associated illicit activities, and ultimately hinder the expansion and improvement of North Korea's sanctioned weapons programs.

Beginning in 2011, and to date, the FATF has recommended financial institutions put in place countermeasures against North Korean financial activities due to its money laundering, terrorist financing, and proliferation financing risks, as well as widespread efforts to evade UN sanctions and national financial laws. North Korea is currently the only jurisdiction where FATF has urged these global countermeasures be put in place, a call renewed in October 2019.[52] In a unilateral

[50] United States District Court in the Southern District of New York, *United States of America v. Ahmad Fathi et. al.*, unsealed in March 2016, https://www.justice.gov/opa/file/834996/download
[51] See: https://www.un.org/securitycouncil/sanctions/1718
[52] FATF, "Public Statement – October 2019."

move, in 2016, the United States designated North Korea a jurisdiction of primary money laundering concern, allowing the Secretary of the Treasury to direct U.S. financial institutions to undertake enhanced countermeasures, including additional required due diligence.[53] The United States previously designated and froze the assets of numerous North Korean banks, bank accounts, and related entities and individuals, located in that country and abroad. Most prominently, in 2005, it froze some $24 million in North Korean assets held by Macau's Banco Delta Asia, generating panic and even economic downturn in North Korea as Pyongyang attempted to repatriate some of the funds.[54]

In comparison to Iran's proliferation finance methods and tactics, North Korea's proliferation financing efforts are more creative in violating laws and norms and more elaborate in their schemes, as well as exploitative of global financial and other regulatory loopholes. North Korea's efforts are also far more centralized, with fewer actors involved and a relative closeness of all "nodes" in a network to a few central financial actors. This is due to the small country's relative isolation, more limited assets, and poor connections to global financial avenues. Its financial cyber-hacking efforts, for example, are run out of the intelligence service, the Reconnaissance General Bureau.[55] An assessment by C4ADS on North Korea's illicit finance system deemed it "centralized, limited, and vulnerable."[56] Its system is centralized due to state ownership of most relevant financial enterprises and the presence of a few well-connected individual and entity facilitators. The report noted the presence of only some 5,233 total companies in North Korea. It is limited because of its vast connections and reliance on China, and vulnerable because disrupting a few key chokepoints can destabilize or stop entire proliferation financing schemes.

The U.S. *National Proliferation Financing Risk Assessment for 2018* pointed out a significant "fundraising element, rather than strict procurement of WMD-related components," used by North Korea. It stated that the United States often finds in the course of investigations that "…the financial facilitators working on behalf of Pyongyang were not attempting to directly acquire sensitive or dual-use goods that can be utilized for weapons development purposes, but rather were engaging in elaborate schemes to evade U.S. and international sanctions to raise funds that can be used to fund the country's illicit weapons programs."[57]

---

[53] *U.S. Federal Register,* Vol. 81, No. 107, June 3, 2016; U.S. Department of Treasury, "Treasury Takes Actions to Further Restrict North Korea's Access to the U.S. Financial System," June 1, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0471.aspx

[54] Patricia Zengerle, "U.S. Takes Further Steps to Block North Korea's Access to Financial System," Reuters. June 1, 2016.

[55] *Report of the Panel of Experts*, August 30, 2019.

[56] C4ADS, *Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System,* 2017, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/59413c8bebbd1ac3194eafb1/1497447588968/Risky+Business-C4ADS.pdf

[57] *National Proliferation Financing Risk Assessment for 2018.*

In March 2019, the UN Panel of Experts on North Korea found that member state implementation of financial measures has not been improving.[58] The Panel's August 2019 report also noted "ongoing deficiencies."[59] The Panel stated that North Korea "enjoys ongoing access to the international financial system, as its financial networks have quickly adapted to the latest sanctions, using evasive methods in ways that make it difficult to detect illicit activity. Member States also continue to fail to take measures required by the Security Council resolutions…"[60] The Panel highlighted the failure by countries to freeze North Korean assets. For example, even if countries would close bank accounts of designated entities, they would allow North Korean individuals or entities to repatriate the funds, including those of the Reconnaissance General Bureau.[61] North Korea also creates revenue-raising joint ventures with other countries that do not adequately enforce sanctions, frequently concealing its own involvement. Governments may or may not be aware of the activity. The UN reporting on North Korea describes that many countries turn a blind eye to North Korea's illicit financial activity, do not enforce UN resolutions, or even when made aware of illicit activity by the Panel, deny or do not stop it.[62]

FinCEN released an advisory in November 2017 stating that North Korea uses one key method in particular to conduct proliferation financing, in this case impacting the U.S. financial system:

> *…North Korean state-owned enterprises [use] foreign based front or shell companies and covert representatives based abroad to obfuscate the true originator, beneficiary, and purpose of transactions, enabling millions of dollars of North Korean illicit financial activity to flow through U.S. correspondent accounts.*[63]

FinCEN stated that North Korea frequently uses "China-based front or shell companies, trading companies, and financial institutions operating in areas bordering the Democratic People's Republic of Korea (DPRK)."[64] These companies facilitate the sale of sanctioned North Korean goods, the purchase of and payment for needed WMD-related goods, and the return of payments to North Korea. FinCEN reported, "the DPRK uses and maintains a network of financial representatives, primarily in China, who operate as agents for North Korean financial institutions." They are able to open bank accounts and establish front companies to facilitate North Korea's illicit business. Once representatives establish a shell company in a country that employs weak corporate establishment practices, they are then able to more easily open bank accounts and conduct financial transactions. 2018 and 2019 UN Panel of Experts reports

---

[58] *Report of the United Nations Panel of Experts established pursuant to Resolution 1874 (2009),* S/2019/171, March 5, 2019.
[59] *Report of the Panel of Experts*, August 30, 2019.
[60] *Report of the Panel of Experts*, March 5, 2019.
[61] Ibid, p. 48.
[62] *Report of the Panel of Experts,* March 5, 2018; *Report of the Panel of Experts*, March 5, 2019.
[63] U.S. Department of Treasury, Financial Crimes Enforcement Network (FinCEN), "Advisory on North Korea's Use of the International Financial System," November 2, 2017, https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf
[64] FinCEN, "Advisory on North Korea's Use of the International Financial System," November 2, 2017.

identified some 30 people who continue to function as these financial representatives, including diplomats.[65] In 2019, the Panel "found those banks to be operating through representatives in China, Indonesia[,] Libya, the Russian Federation, the Syrian Arab Republic and the United Arab Emirates." The Panel described how North Korea relies heavily on China, Hong Kong, Malaysia, Russia, broader Asian region, and Middle Eastern entities to facilitate its proliferation financing and raising of revenues. Notably, when faced with specific Panel information about individuals engaged in North Korean illicit financing on Chinese territory, China frequently responded that the North Koreans in question did not fall under United Nations sanctions or that it had no knowledge of the activities. However, the Panel found that the representatives in China were "subject to expulsion under paragraph 33 of resolution 2321 (2016)."[66] China's inaction as one of North Korea's predominant financing partners is a key reason why North Korea is able to continue funding its proliferation programs.

North Korea utilizes official government employees, diplomats, diplomats' family members, foreign embassy personnel, and intelligence bureau officers to carry out many of its illegal financial endeavors; its embassies abroad are known for facilitating those criminal activities.[67] FinCEN wrote in its advisory, "Various financial representatives and corporate service providers may establish…front or shell companies or serve as representatives of the various involved entities."[68] North Korea's revenue-raising schemes operate like a quasi-state mafia with a few at the top directing and reaping the principal benefits. "Office 39," for example, started in the 1970s, directs many illicit revenue-raising activities and maintains the regime's foreign currency and reserve funds. State-directed companies are mere enablers of these illicit activities, allowing North Korea to stretch abroad the tentacles of its efforts. Office 39 runs "a network of companies around the world involved in both illegal and legal trade and is estimated to bring in between $US500 million and $US2 billion a year into North Korea."[69] A defector who worked for Office 39 claimed in a media report that evading UN sanctions was easy to do where there is an absence of sanctions enforcement. "You just change company names and have branches in other countries," he stated.[70] He claimed that as the world becomes more aware of North Korea's illicit efforts, however, the task of Office 39 was becoming more difficult. North Korea also relies on the smuggling of bulk cash. It is occasionally caught using the diplomatic pouch to move hard currency to or from foreign countries.[71] North Korea draws revenue from workers abroad, carries out foreign projects, and trains foreign military units, all banned under UN sanctions.[72]

---

[65] *Report of the Panel of Experts*, March 5, 2018, p. 4; *Report of the Panel of Experts*, August 30, 2019.
[66] *Report of the Panel of Experts*, March 5, 2018, Annex 43.
[67] *Report of the Panel of Experts,* March 5, 2018.
[68] FinCEN, "Advisory on North Korea's Use of the International Financial System," November 2, 2017.
[69] Matthew Carney, "Defector Reveals Secrets of North Korea's Office 39, Raising Cash for Kim Jung Un," *ABC (Australia) News,* January 5, 2018.
[70] Ibid.
[71] Ibid.
[72] See, for example, more on how North Korean workers are employed in Uganda, and how North Korea trains military units in Uganda for funds, despite Uganda stating that it would end such cooperation: Joe Parkinson, "Never Take Their Photos: Tracking the Commandos, North Korea's Secret Export," *The Wall Street Journal,* December 9, 2018.

North Korea increasingly pursues virtual means of raising capital for proliferation related to its nuclear, missile, and arms programs. In about 2013, North Korea began the "pioneering work" of carrying out state-led cyber-attacks and use of malware to steal funds.[73] North Korea's APT38 and Lazarus Group cyber-hacking entities began attacking banks, virtual currency exchanges, and a variety of other types of businesses. In its August 2019 report, the UN Panel wrote, "A Member State informed the Panel that the proportion of revenue received from attacks by Democratic People's Republic of Korea cyber actors has grown in relation to income generated through other activities."[74]

The Panel also noted the rise of North Korean attacks on cryptocurrency exchanges, use of ransomware to demand cryptocurrency payments, and mining or "cryptojacking" of cryptocurrency to steal millions of dollars since at least 2017.[75] In its August 2019 report, it detailed one identified attack to steal cryptocurrency:

> *…Attackers use a digital version of layering in which they create thousands of transactions in real time through one-time use cryptocurrency wallets. According to [a] Member State, stolen funds following one attack in 2018 were transferred through at least 5,000 separate transactions and further routed to multiple countries before eventual conversion to fiat currency, making it highly difficult to track the funds.*[76]

North Korea also stated an intention to create its own cryptocurrency exchange to circumvent sanctions.[77] Although North Korea's shocking cyber-hacking efforts have led to the issuance of new guidance and alerts by authorities to guard against North Korean schemes, many countries, as well as the private sector more broadly, lag in setting up adequate cyber defenses against its aggressive malware and attacks.[78]

Other non-traditional means of raising revenue include North Korea's sales of key minerals, coal, and textiles, which are banned by UN sanctions and raise capital for the purchase of nuclear, missile, and military-related goods. Resolution 2371 (2017) attempted to prevent North Korea's sales of commodities, such as coal and seafood, that have been observed to fund its proliferation programs. However, North Korea has evaded this restriction on its ability to deliver coal to Chinese, Russian, and other ports by simply carrying out "regularizing and systematic," evasive ship-to-ship transfers at sea, as described by the Panel of Experts in its

---

[73] Choe Sang-Hun, "Computer Networks in South Korea are Paralyzed in Cyberattacks," *The New York Times,* March 20, 2013, https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html
[74] *Report of the Panel of Experts,* August 30, 2019, p. 23.
[75] Ibid, pp. 26-30.
[76] Ibid, p. 27.
[77] David Gilbert, "North Korea is Building its Own Bitcoin," *Vice News,* September 18, 2019, https://www.vice.com/en_us/article/9ke3ae/north-korea-is-building-its-own-bitcoin
[78] Rishi Iyengar, "How North Korea is Hacking Companies and Governments," CNN, November 15, 2017, https://money.cnn.com/2017/11/15/technology/north-korea-hacking-fallchill-volgmer-fbi-dhs/index.html

March 2019 report.[79] A Member State informed the Panel of Experts that such observed coal trade activities "comprise only one element of much larger trades of commodities from the [DPRK] that involve unwitting international banks providing letters of credit to a wider, transnational trading network that operates through offshore jurisdictions such as the British Virgin Islands and in Hong Kong, China, as well as other locations."[80]

The targeted UN sanctions on North Korea's trade in proliferation revenue-raising commodities have had an effect, particularly the prohibitions on its main export of coal.[81] Economic analysis by the Observatory of Economic Complexity at Massachusetts Institute of Technology (MIT) found that North Korean exports to China had decreased from $2.3 billion in 2016 to $1.58 billion in 2017.[82] However, experts note that North Korea's growing trade deficit with China may be financed via trade that is simply undocumented and circumvents the sanctions.[83] For example, even though China halted overt imports of North Korean coal in February 2017, both China and Russia have been observed quietly importing coal in violation of sanctions, both via rail and sea.[84] Propped up by these two key trading partners, North Korea manages to find other unwitting partners and workarounds to continue raising enough revenue to keep its economy, and ultimately its weapons programs, afloat. According to the U.S. *National Proliferation Financing Risk Assessment for 2018*: "Although U.S. and international sanctions have significantly hampered North Korean [proliferation financing] schemes, the North Korean government continues to adapt and use creative methods to access the international, and in many cases the U.S., financial system."[85] North Korea also relies on currency counterfeiting, drug sales, pharmaceutical counterfeiting, cigarette counterfeiting, sales of conflict diamonds and gold, and other means to raise funds for proliferation-relevant activities.[86]

Overall, despite its more limited means of doing so and comparative isolation, North Korea has succeeded over the decades in augmenting its nuclear, missile, and military systems, which means that payments for illicit procurements are getting through successfully and money is flowing to the regime to support those programs. The March 2019 Panel of Experts report showed that 56 countries were involved in UN sanctions violations throughout the reporting

---

[79] *Report of the Panel of Experts*, March 5, 2019, p. 21, Annex 15.
[80] Ibid, p. 26.
[81] Observatory of Economic Complexity, "What Does North Korea Export? (1995-2017), Massachusetts Institute of Technology, https://atlas.media.mit.edu/en/
[82] Observatory of Economic Complexity, Massachusetts Institute of Technology, "Where Does North Korea Export To? (1995-2017)," https://atlas.media.mit.edu/en/
[83] Ben Heubl, "North Korea's Mysterious Trade Deficit with China – in Charts," *Nikkei Asian Review,* October 8, 2018, https://asia.nikkei.com/Spotlight/Datawatch/North-Korea-s-mysterious-trade-deficit-with-China-in-charts
[84] Chen Aizhu, "Exclusive: China's CNPC Suspends Fuel Sales to North Korea as Risks Mount – Sources," Reuters. June 28, 2017, https://finance.yahoo.com/news/exclusive-chinas-cnpc-suspends-fuel-012344827.html ; Peter Makowsky, Jenny Town, and Samantha Pitz, "A Snapshot of North Korea's Supply Chain Coal Activity – Part II," *38North,* April 1, 2019, http://go.pardot.com/e/394142/2U7hUWy/j3hv24/674268745?h=_-vk0_csbhJehFtynxF2Axiu6u8NcpxDZWTh9AMKpsk
[85] *National Proliferation Financing Risk Assessment for 2018.*
[86] Joshua Berlinger and Zachary Cohen, "The Secrets Behind Kim Jong Un's Personal Piggy Bank," CNN, June 20, 2017; Mark Gollom, "Drugs, Counterfeiting: How North Korea Survives on Proceeds of Crime," *CBC*, December 7, 2017.

period.[87] Twenty-eight countries were involved in non-military-related cases of alleged business and financial-related sanctions violations that involved joint ventures, facilitating activities of front companies, financial transaction enablement, employment of North Korean nationals, travel violations, construction contracts, brokering, and allowing North Korea to use property for commercial purposes. Notably, some of the cast of countries changes by year according to the UN reporting, supporting the view that North Korean proliferation financiers continue to probe for weaknesses in sanctions implementation and enforcement if schemes are uncovered and stopped. They exploit new opportunities as available.

[87] David Albright, Sarah Burkhard, Bernadette Gostelow, Maximilian Lim, and Andrea Stricker, "56 countries involved in violating UNSC Resolutions on North Korea during last reporting period," *Institute for Science and International Security*, June 6, 2019, http://isis-online.org/isis-reports/detail/56-countries-involved-in-violating-unsc-resolutions-on-north-korea-during-t

Chapter 6. Iranian Case Studies

A series of case studies follows in the next two chapters which demonstrate several of the warning signs and methods, with a focus on Iranian and North Korean illicit financing schemes to finance their sanctioned nuclear, other WMD, missile, and military programs. These are two of the most problematic countries with regard to threats to the United States and broader counter-proliferation efforts, as identified by the U.S. intelligence community's unclassified *Worldwide Threat Assessment for 2018*.[1]

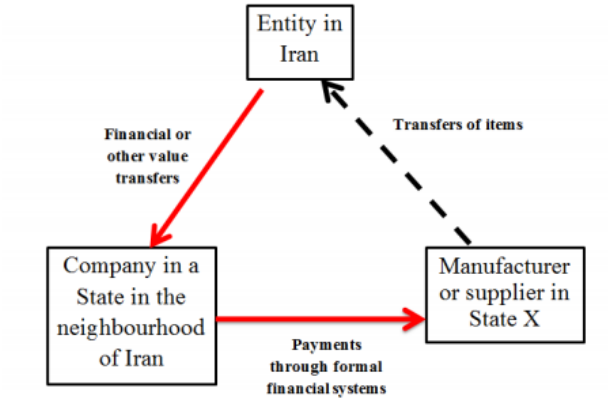
Case 6.1: Iran's Movement of Funds Using Formal Financial System/Offset Payments Scheme

The former UN Panel of Experts on Iran established pursuant to Resolution 1929 (2010) closely investigated Iran's illicit finance for its nuclear, missile, and military programs. With the implementation of the nuclear deal in 2016, all prior UNSCRs against Iran were terminated, and the work of the Panel was ended. Its findings, however, remain relevant particularly with the reinstatement of U.S. financial sanctions. In the Panel's final report, it explained a common method Iran uses to move money, as relayed to them by a member state: "A local company needed to pay for services provided by an Iranian entity, but was unable to do so because the entity was designated under national legislation. Instead, the local company made offset payments to domestic manufacturers for spare parts they had previously supplied to the Iranian entity."[2] This method is described in Figure 6.1.

[1] Statement of Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community,* 2018, pp. 7-8, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

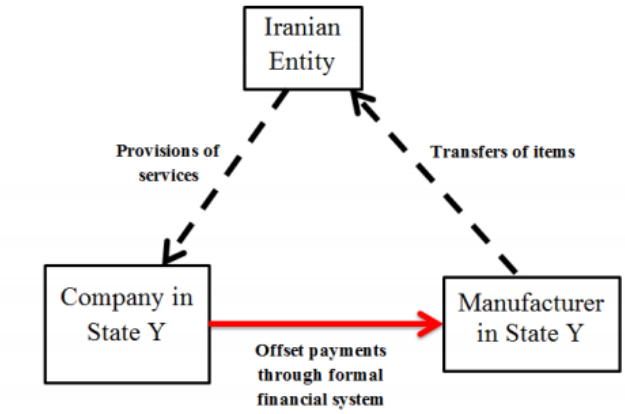
[2] *Report of the Panel of Experts established pursuant to Resolution 1929 (2010),* S/2015/401, June 2, 2015.

Figure V
Illustration of possible methods used by Iranian entities to finance procurement*



* These methods could be used for both legitimate procurement and for procurement prohibited under Security Council resolutions relating to the Islamic Republic of Iran.

Figure VI
Illustration of a variant of figure VI*



* In exchange for services received from an Iranian entity, a company abroad makes payments to a manufacturer for goods it supplied to that Iranian entity.

Figure 6.1. Iran's method of using offset payments through the formal financial system to fund purchases. From: *Report of the Panel of Experts established pursuant to Resolution 1929 (2010),* S/2015/401, June 2, 2015.

Case 6.2: Iran's Use of Foreign Exchange Houses to Obtain Dollars

FinCEN closely tracks Iran's efforts to finance its acquisition of commodities for its nuclear, missile, military, and other sanctioned programs. An October 2018 advisory for financial institutions, *Advisory on the Iranian Regime's Illicit and Malign Attempts to Exploit the Financial System,* explains how Iran increasingly uses foreign exchange houses to circumvent restrictions on its ability to trade and pay for goods in dollars. In May 2018, the United States and the UAE "disrupted an extensive currency exchange network in Iran and the UAE. The network procured

then transferred millions of U.S. dollar-denominated bulk cash through the UAE to the IRGC-QF."[3] Figure 6.2 shows how Iran's exchange house scheme functioned:

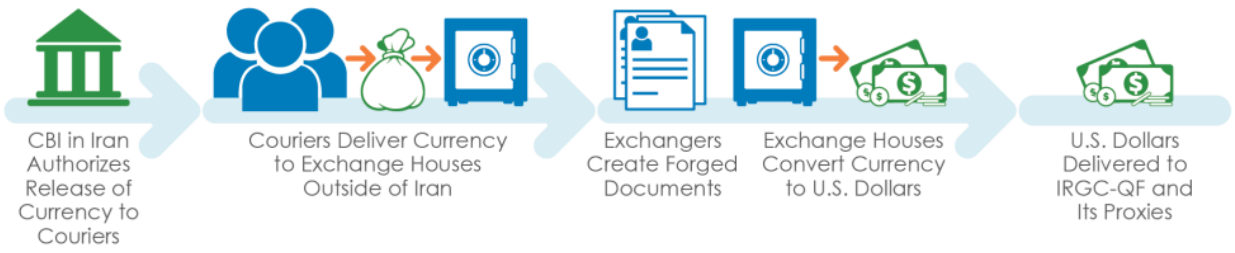


Figure 6.2. Credit: FinCEN, "Advisory on the Iranian Regime's Illicit and Malign Attempts to Exploit the Financial System," October 11, 2018.

The CBI helped the IRGC-QF carry out the scheme. The IRGC-QF first established three front companies, or exchange houses, in the UAE. As Figure 6.2 explains, the CBI would deliver via courier cash currency to the exchange houses in the UAE. Then, "using the front companies, these individuals and entities procured and transferred millions in U.S. dollar-denominated bulk cash to the IRGC-QF to fund its malign activities and regional proxy groups." The advisory noted, "These third-country exchange houses or trading companies frequently lack their own U.S. dollar accounts and instead rely on the correspondent accounts of their regional banks to access the U.S. financial system." The UAE-based exchanges helped facilitate the creation of forged documents and converted the currency into U.S. dollar-denominated bulk cash. Those involved in the scheme were sanctioned by the United States.[4]

Case 6.3: Iran's Acquisition of Majority Shares in Foreign Banks

In addition to facilitating illicit procurement and a variety of its malign regional activities, Iran's illicit financing schemes seek to carry out government-origin monetary transfers. The former UN Panel of Experts on Iran, in its final report of June 2015, for example, observed that in 2011, Iranian officials were acquiring majority shares in foreign banks, "which [were] then used to facilitate transactions through several Iranian banks including Bank Melli and Bank Saderat."[5]

Case 6.4: Iran's Repatriation of Funds Held Up in Foreign Banks

In one case in which Iranian oil funds were held up at foreign banks, a UN member state reported a scheme to the Panel of Experts in which:

---

[3] FinCEN, "Advisory on the Iranian Regime's Illicit and Malign Attempts to Exploit the Financial System," October 11, 2018.

[4] U.S. Department of Treasury, Press Release, "United States and United Arab Emirates Disrupt Large Scale Currency Exchange Network Transferring Millions of Dollars to the IRGC-QF," May 10, 2018, https://home.treasury.gov/news/press-releases/sm0383

[5] *Report of the Panel of Experts,* June 2, 2015, p. 21.

Several Iranians holding student visas set up eight separate shell companies in the State concerned in 2013 and 2014 in order to access at least $150 million of oil export revenues in accounts held by the Central Bank of the Islamic Republic of Iran at a State-owned bank. The funds were reportedly paid out against invoices for exports of goods to the Islamic Republic of Iran, although the goods were never exported.[6]

FinCEN also warned that it "has repeatedly observed CBI officials and the IRGC-QF using regional financial institutions as intermediaries to conceal illicit transactions." The CBI uses IRGC-QF front companies to "retrieve funds – some which are generated by the sale of Iranian oil – in various currencies from foreign bank accounts held by the CBI and then transfer[s] funds back to Iran."[7]

Case 6.5: Use of Central Bank of Iran to Conduct Terrorist Financing

FinCEN also explained key ways in which Iran tries to undermine the integrity of the U.S. and global financial system, for example, "misusing exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, including those at the Central Bank of Iran."[8]

In one case observed by FinCEN, senior officials of Iran's sanctioned Central Bank used "their official capacity to procure hard currency and conduct transactions for the benefit of the IRGC-QF (Islamic Revolutionary Guards-Quds Force) and its terrorist proxy group, Lebanese Hizballah. In May 2018, Treasury's OFAC designated two such officials for moving "millions of dollars, in a variety of currencies, through the international financial system…"[9] It also designated the Chairman of another bank, al-Bilad Islamic Bank of Iraq, which "acted as an intermediary to enable and conceal those transactions."

Case 6.6: How Financial Conspiracy Charges Against Iran's Shipping Line Disrupted Illicit Shipping and Financing Operations

Iran frequently exploits its national shipping lines as assets to move money relevant to its proliferation activities. On June 21, 2011, the District Attorney (DA) of Manhattan announced a 317-count indictment against the Iranian government-owned shipping lines, Islamic Republic of Iran Shipping Lines (IRISL), and several of its affiliates and aliases.[10] The indictment charged that between September 2008 and January 2011, IRISL and three affiliates operating out of Singapore, the UAE, and Britain, seven other companies or aliases, and five individuals

[6] Ibid.
[7] FinCEN, "Advisory on the Iranian Regime's Illicit and Malign Attempts to Exploit the Financial System," October 11, 2018.
[8] Ibid.
[9] Ibid.
[10] District Attorney for New York County, "DA Vance Announces Indictment of Iranian Shipping Line for the Illegal Use of Banks in Manhattan," June 20, 2011, https://www.manhattanda.org/da-vance-announces-indictment-iranian-shipping-line-illegal-use-banks-manhattan/

committed conspiracy to circumvent United States sanctions against Iran by illegally accessing New York banking institutions to send and receive more than $60 million in payments.[11]

National and international sanctions against IRISL and its affiliates are, as the U.S. indictment indicated, "…designed to interrupt IRISL's business operations" insofar as they serve the needs of Iran's WMD programs. The indictment stated, "These restrictions [present] significant problems for IRISL because, without access to U.S. financial institutions, IRISL could not make or receive U.S. dollar payments relating to its commercial activities."[12]

In September 2008, the United States added IRISL and 15 related entities, in addition to 123 IRISL vessels, to the Specially Designated Nationals List (SDN List) for their involvement in transporting or proliferating WMD.[13] Three of the IRISL affiliates sanctioned in 2008 were indicted by the New York DA: Asia Marine Network Pte Ltd., located in Singapore; Oasis Freight Agencies, located in the UAE; and Irinvestship Ltd, located in Britain. Their aliases and operators were also indicted. Between August 2010 and February 2011, the United States designated an additional 109 individuals and entities relating to IRISL and several more vessels. The EU also designated IRISL entities associated with Iran's WMD proliferation activities in July 2010. The designated entities are forbidden from accessing U.S., and formerly, EU banks.

In March 2008, the United Nations Security Council passed resolution 1803, now terminated, which called upon member states to "inspect the cargoes to and from Iran, of aircraft and vessels, at their airports and seaports, owned or operated by…Islamic Republic of Iran Shipping Line…" if there were reason to believe WMD related materials were aboard.[14] Resolution 1929, passed in June 2010, sanctioned three affiliates of IRISL and called upon member states to communicate "any information available on transfers or activity by…vessels owned or operated by the IRISL to other companies that may have been undertaken in order to evade the sanctions of, or in violation of the provisions of, resolutions 1737 (2006), 1747 (2007), 1803 (2008) or this resolution, including renaming or re-registering of aircraft, vessels or ships…"[15]

The Scheme

Following its sanctioning, IRISL took steps to obscure the actual ownership of its vessels by creating "a web of shell companies stretching across Europe and Asia," according to an investigative piece by *The New York Times*.[16] It regularly changed ships' flag names and the names of the companies or individuals operating them, even moving entire shipping industries under new names "virtually overnight" according to records seen by *The Times*. A *Times* visit to

[11] *Indictment: People of the State of New York vs. Islamic Republic of Iran Shipping Lines et. al.*
[12] Ibid.
[13] "DA Vance Announces Indictment of Iranian Shipping Line for the Illegal Use of Banks in Manhattan."
[14] UNSC, *Resolution 1803 (2008),* http://www.isisnucleariran.org/assets/pdf/unsc_res1803.pdf
[15] UNSC, *Resolution 1929 (2010)*, https://www.iaea.org/sites/default/files/unsc_res1929-2010.pdf
[16] Jo Becker, "Web of Shell Companies Veils Trade by Iran's Ships," *The New York Times*, June 7, 2010, https://www.nytimes.com/2010/06/08/world/middleeast/08sanctions.html?scp=2&sq=irisl&st=cse

the given address of one entity under indictment by the United States, Hafiz Darya Shipping Lines (HDS Lines), located in Tehran, revealed that the address was a club used by IRISL employees. Upon further investigation, Hafiz Darya Shipping Lines and another indicted entity, Sapid Shipping Co., were actually located at IRISL headquarters. The managers of the various entities were found to be high-level IRISL employees.

The result of this maneuvering was that blacklists could not keep up with the "camouflage" used by the sanctioned entities, which handicapped financial transaction screening systems designed to detect illicit financial transactions by IRISL-owned or -affiliated entities. The scheme is described in Figure 6.3 below. It shows how IRISL affiliates located in third-party countries that were the target of U.S. sanctions established new entities to conduct illicit financial transactions. These entities were located in countries other than Iran that were not subject to sanctions, which obscured their origin. They successfully carried out millions of dollars in transactions via New York county banks before the scheme was uncovered.

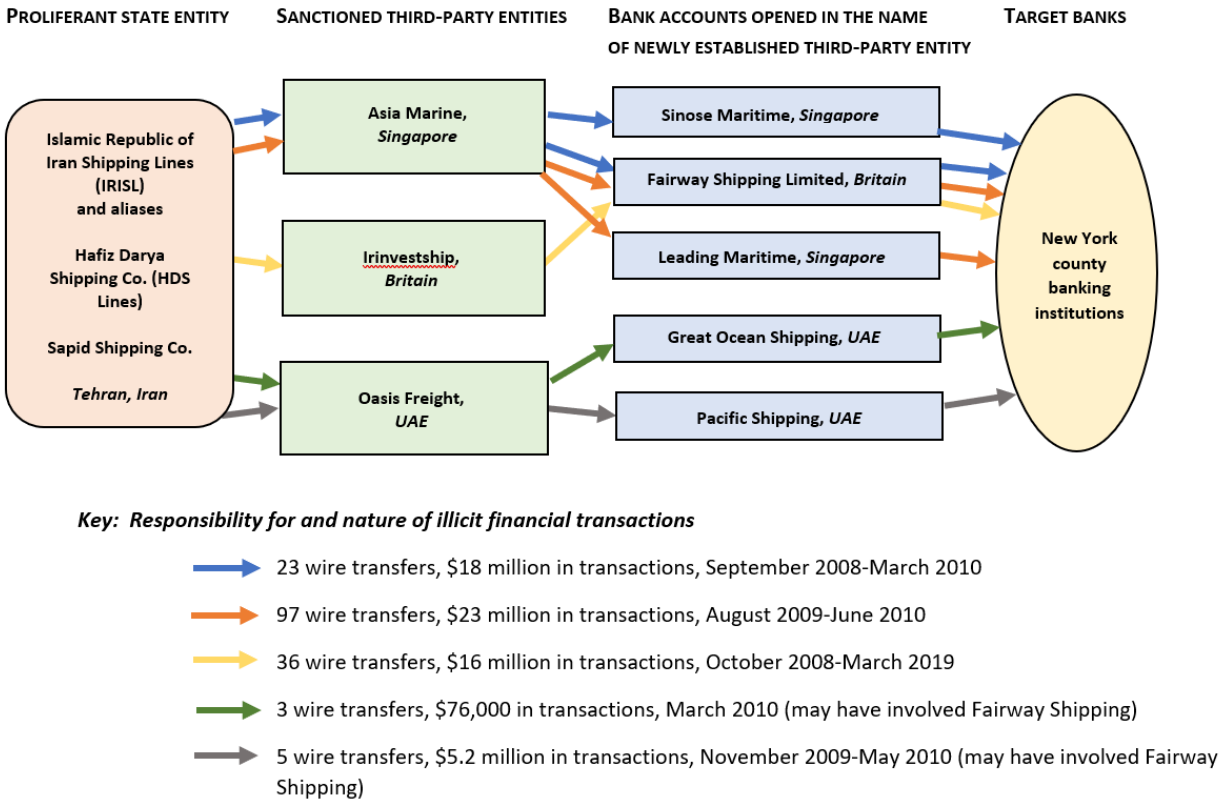


Figure 6.3. Representation of the scheme used by IRISL and its affiliates to defraud New York county banking institutions.

Case 6.7: U.S. Authorities Detect Chinese-State Sanctioned Illicit Financing Scheme Aimed at Enabling Iran's Nuclear and Missile Procurements

From November 2006 to September 2008, Li Fang Wei, a Chinese citizen and the owner of Limmt Economic and Trade Company, Ltd. located in Dalian, China, allegedly illegally procured for Iran equipment and materials usable in nuclear, ballistic missile, or conventional military programs. The New York District Attorney's office charged that his procurements were in violation of United Nations resolutions and NSG and MTCR export guidelines, and that he used the United States financial system to receive payment for these illicit procurements.[17] In June 2006, Limmt was sanctioned by the U.S. Treasury Department for activities relating to WMD procurement and blacklisted from accessing the U.S. financial system. Despite this, Limmt and its owner, using company aliases and phony names, allegedly continued to route payment transactions through New York state bank accounts for procurements made for Iran.

High-level U.S. officials opened discussions with China about Limmt's activities in February 2006, but became frustrated with China's inaction. In April 2009, a New York State Grand Jury moved to indict Limmt and Li Fang Wei and charge them with conspiracy in the fifth degree and one hundred and eighteen counts of deception and fraud against United States financial institutions, eight counts which involved Iranian customers. In light of the fact that the United States and the People's Republic of China do not have an extradition treaty, Li has not faced prosecution in the United States for his crimes. China has still not agreed to extradite Li.

The Scheme

Limmt Economic and Trade Company is a metallurgical production and trading firm which serves international customers in sales of metal alloys and minerals. It allegedly runs a side business in illicit procurement of dual-use materials for entities of the Iranian military establishment affiliated with the state's nuclear, missile, and conventional military programs. OFAC's SDN List, to which Limmt was added in June 2006, bans it from accessing the U.S. financial system and prohibits U.S. companies from doing business with the firm. U.S. financial institutions blocked several attempted transactions associated with Limmt immediately after it was added to the SDN List.

In August 2006, shortly after the Treasury Department sanctioned Limmt for its proliferation activities, Limmt allegedly attempted to complete a financial transaction in the amount of $40,000 through Citibank in New York. Citibank's screening systems detected this transaction. Once Limmt became aware that U.S. banks were rejecting or freezing the company's transactions due to the sanctions, it allegedly began setting up bank accounts under phony company names, obscuring sales records, and attempting to hide the country origin of payments to its accounts.

[17] Supreme Court of the State of New York, *Indictment, The People of the State of New York against Li Fang Wei and Limmt Economic Trade Company (and aliases),* April 7, 2009.

Subsidiaries or entities acting on behalf of the Iran Defense Industries Organization (DIO) (known in Persian as "Sazemane Sanaye Defa" or "SSD"), allegedly purchased from Limmt a range of sensitive materials, including graphite, tungsten copper, tungsten powder, high strength aluminum alloys, and maraging steel.[18] These goods are controlled by international conventions and national export control regimes because of their potential application in nuclear, ballistic missile, and military programs. DIO directs many of the Iranian military establishment's overseas illicit procurement activities. It was sanctioned by the U.S. Treasury Department in March 2007 for engaging in WMD proliferation.

These subsidiaries or entities placed orders with Limmt for needed goods and paid for the purchases upon receipt of special account and payment instructions, in which Limmt would allegedly specify account details at New York banks held under aliases and provide instructions to Iranian entities on how to route payments undetected. Limmt allegedly sent banned goods to several companies linked to DIO including: Khorasan Metallurgy Industries, Amin Industrial Group, Shahid Sayyade Shirazi Industries, Yazd Metallurgy Industries, and Aban Commercial and Industrial Company. Eight procurements and associated financial transactions with Iranian entities are detailed in the indictment of Limmt and Li Fang Wei which involve illegal access to the U.S. financial system (see Figure 6.4 below, which shows the routes of payments for procurements made on behalf of Iran). Li and Limmt are also under indictment for several dozen other illegal financial transactions involving non-Iranian clients, accounting for the total one hundred and eighteen fraud and deception charges.

In November 2006, Li Fang Wei informed an Iranian customer that Limmt had been added to the "black lists of USA treasury ministry due to some business activities with your several large governmental organizations/companies."[19] He stipulated that in the future, Limmt would go by the name "Sino Metallurgy and Minmetals Industry Co., Ltd." Limmt allegedly went on to use several other aliases to set up its bank accounts at New York financial institutions. According to the indictment, Limmt's other aliases for financial transactions and phony company names for shipping to Iranian entities included: Blue Sky Industry Corporation, SC (Dalian) Industry and Trade Co., Ltd., Rwiot Steel Service; Sunny Minerals Company Limited, Wealthy Ocean Enterprises, Ltd., and Liaoning Industry and Trade Co., Ltd.

[18] According to the May 2009 testimony before the Senate Foreign Relations Committee of then-New York District Attorney Robert M. Morgenthau, Limmt and the DIO were also negotiating the sale of gyroscopes, accelerometers, and tantalum. Morgenthau stated, "gyroscopes and accelerometers are crucial technology for Iran's development of long range missiles, and tantalum in the form indicated can be used to manufacture armor-piercing projectiles of the sort found in improvised explosive devices (IEDs)." Testimony transcript is available at: http://foreign.senate.gov/testimony/2009/MorgenthauTestimony090506a.pdf

[19] *Indictment, New York against Li Fang Wei and Limmt,* April 7, 2009.

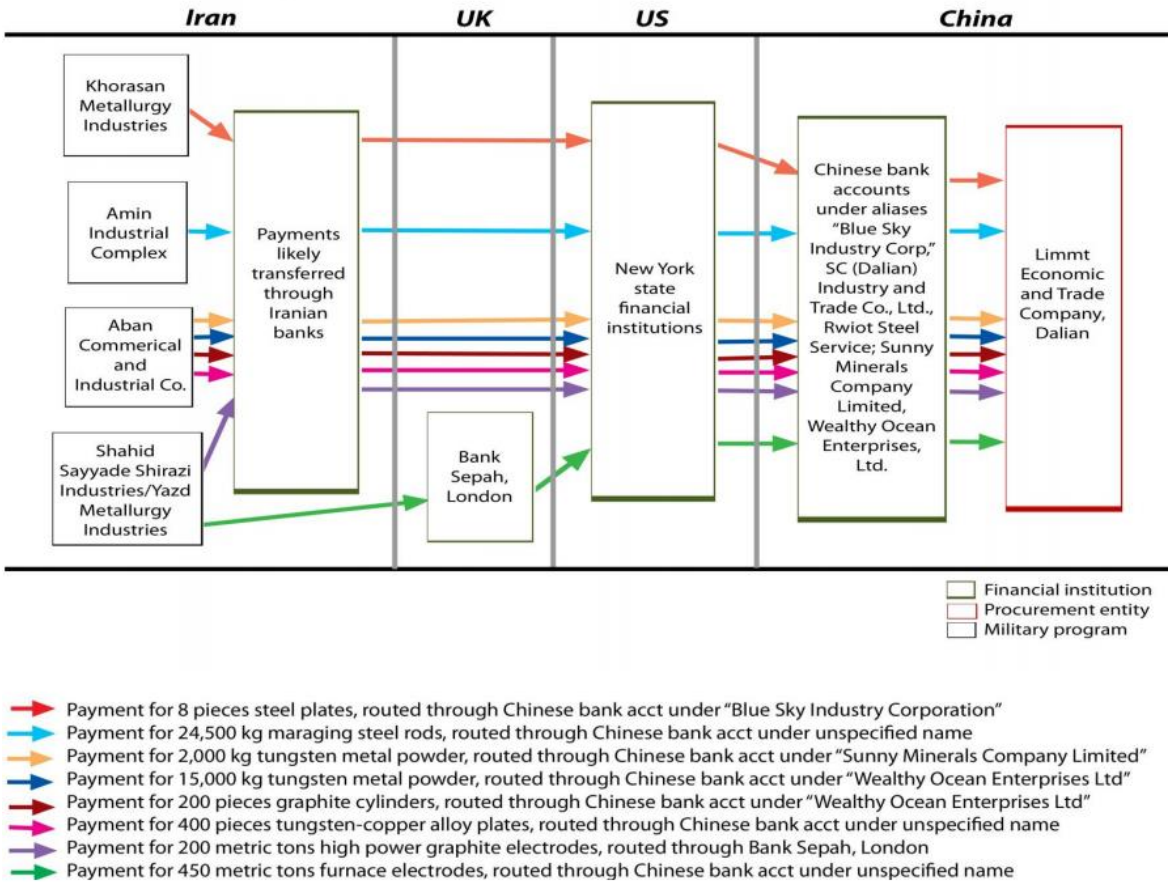


Figure 6.4. Payment routes for series of goods illicitly financed for Iran by Li and Limmt via the U.S. financial system.

Case 6.8: How Extraterritorial Enforcement Can Disrupt Iran's Illicit Financing Schemes – Example of Huawei and Skycom[20]

On December 1, 2018, Canadian officials arrested the Chief Financial Officer (CFO) of Huawei, a major Chinese telecommunications company, following a U.S. provisional arrest warrant request. Meng Wanzhou was accused by the United States of committing financial fraud charges that violated U.S. sanctions against Iran. The United States gave Canada information leading to the arrest of Meng as she entered a Canadian airport, and is seeking her extradition pursuant to their mutual extradition treaty. The Canadian affidavit detailing the circumstances behind Meng's arrest alleges that Meng was part of a conspiracy by Huawei to run what was allegedly a front company used to process financial transactions to Iran. The company, Skycom Tech, a Hong Kong and Iran-based entity that authorities say was controlled by Huawei,

[20] Andrea Stricker, "Case Study: How Extraterritorial Enforcement Can Disrupt Iran's Illicit Financing Schemes - the Example of Huawei and Skycom," *Institute for Science and International Security*, December 13, 2018 http://isis-online.org/isis-reports/detail/case-study-how-extraterritorial-enforcement-can-disrupt-irans-illicit-finan/

allegedly funneled money and loans to Iran from two British banks, HSBC and Standard Chartered, as well as other major financial institutions.[21] Meng was accused of hiding Huawei's relationship to Skycom in order to facilitate these transactions.

The Wall Street Journal reported that in addition to major transactions with Huawei by HSBC and Standard Chartered, Citigroup Inc., Australia & New Zealand Banking Group Ltd., DBS Group Holdings Ltd., and Bank of China were also major transaction partners with Huawei, meaning that, if these allegations are proven true, their funds may have ended up in Iran.[22] U.S. authorities, including the Federal Bureau of Investigation and Treasury Department, have been investigating Huawei's business dealings with Iran since at least 2017, and the Commerce Department issued an administrative subpoena against it in 2016.[23] Meng has been released from jail on bail pending the conclusion of extradition proceedings.[24] As of this writing, she had not yet been extradited.

Skycom Not Distinct from Huawei

According to the Canadian affidavit based on the U.S.-provided information, Meng served on the board of Skycom Tech from 2008 to 2009.[25] The affidavit states, "According to the financial statements for Skycom for the years 2009 and 2010, the 'principal activities of Skycom were engaged in [sic] investment holding and acting as a contractor for contracts undertaking [sic] in Iran." Furthermore, "former employees of Skycom have stated, in sum and substance, that Skycom was not distinct from Huawei…" Skycom employees allegedly "had Huawei email addresses and badges, individuals working in Iran used different sets of stationary…for different business purposes, and the leadership of Skycom in Iran were Huawei employees." The affidavit notes, "Skycom official documents, including several Memoranda of Understanding, bore the Huawei logo." Documents gathered by law enforcement show that "multiple Skycom bank accounts were controlled by Huawei employees, and Huawei employees were signatories on these accounts between 2007 and 2013." Allegedly, "Managing Directors" for Skycom were in reality Huawei employees. In 2009, Skycom was purportedly "sold" to another entity, but investigators found that this entity was actually controlled by Huawei until at least 2014.

A Reuters investigation in 2013, which analyzed corporate and other records, found that Meng was allegedly involved in another illicit deal between Huawei, aka Skycom, and Iran. Reuters

---

[21] Margot Patrick and Eva Dou, "Two British Banks Ensnared in Huawei Dispute," *The Wall Street Journal,* December 9, 2018.
[22] Ibid.
[23] Sheridan Prasso, "Huawei Probe Adds to U.S.-China Trade Tension Ahead of Talks," *Bloomberg,* April 25, 2018.
[24] Julia Horowitz, Alberto Moya, and Scott McLean, "Facing Extradition to the US, Huawei's CFO is Released on Bail in Canada," CNN, December 12, 2018.
[25] Supreme Court of British Columbia, *Affidavit in the Matter of the Extradition Act and the Matter of the Attorney General of Canada on behalf of the United States of America and Wanzhou Meng,* Court File 27761, dated November 30, 2018, https://www.scribd.com/document/395185754/Surrey-RCMP-Const-Winston-Yep-s-affidavit?utm_source=Risky+Business%3A+Huawei%27s+Iran+Business+Dealings+Catch+Up+With+Them&utm_campaign=UANI+Berlin+Event+3%2F19&utm_medium=email

first revealed the alleged nature of Skycom's business dealings and Huawei's role.[26] At that time, Skycom was implicated in a scheme to sell Hewlett-Packard equipment to Iran. Documents related to the transaction were allegedly marked with Huawei's logo and stamped "Huawei confidential." Reuters also found that in 2007, "a management company [Hua Ying Management Co. Ltd.] controlled by Huawei's parent company held all of Skycom's shares." It noted, "At that time, Meng served as the management firm's company secretary." Prior to and following that, various individuals and "off-shore companies" with direct or indirect ties to Huawei were majority shareholders. In spite of its alleged trade and financing relationship with Iran, Huawei told Reuters that its "business in Iran is in full compliance with all applicable laws and regulations including those of the UN."

Allegedly Moved Money for Iran

The Canadian affidavit states that Meng and Huawei "repeatedly lied about the nature of the relationship between Huawei and Skycom and the fact that Skycom operated as Huawei's Iran-based affiliate in order to continue to obtain banking services from multinational financial institutions."[27] The court filing notes that the motivation for allegedly hiding the nature of Skycom was to avoid U.S., and formerly, European Union sanctions on Iran and to be able to process dollar or euro-clearing transactions. As a result, an entity labeled "Financial Institution 1" in the affidavit, revealed by Ms. Meng's lawyer to be HSBC,[28] allegedly processed "more than $100 million in financial transactions related to Skycom through the United States between approximately 2009 and 2014." HSBC was already under investigation for U.S. sanctions violations and had entered into a deferred prosecutions agreement.

Following the Reuters investigation, in September 2013, HSBC asked Huawei about the content of the allegations made in the articles. Allegedly, Huawei extensively denied the links to Skycom/Iran. Meng was allegedly involved in those misrepresentations and authorities gathered considerable oral and written supporting information indicating so. The affidavit stated, "Financial Institution 1 [HSBC] risk committees relied in part on Meng's representations to continue banking Huawei." The affidavit concluded, "Some of these misrepresentations were made, involved, or resulted in interstate and foreign wire transmissions."

[26] Steve Stecklow, "Exclusive: Huawei CFO Linked to Firm that Offered HP Gear to Iran," Reuters. January 31, 2013.
[27] *Affidavit,* Court File 27761, Dated November 30, 2018.
[28] "Two British Banks Ensnared in Huawei Dispute."

Chapter 7. North Korean Case Studies

Case 7.1: North Korea's Sale of Natural Resources Facilitates WMD and Missile Commodity Purchases

FinCEN explained one frequently used North Korean trade-based scheme to facilitate its illicit WMD and missile financing activities.[1] North Korea sells natural resources to China-based companies, and then the companies sell the natural resources principally in Asia. Next, to return payments to North Korea, the China-based companies "divide their payments into smaller outflows in a complex layering scheme directed to front companies, shell companies, shipping or trade businesses based in Asia (often registered in Hong Kong), and other companies based in various offshore jurisdictions (e.g., British Virgin Islands, Marshall Islands, and the Seychelles)."[2] FinCEN illustrates this type of scheme in a graphic:

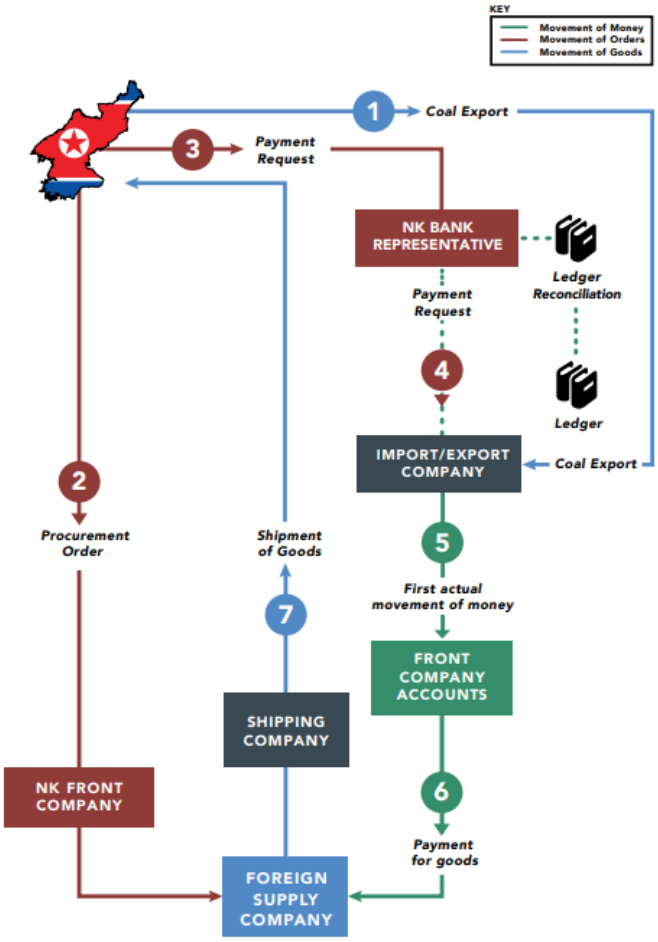


Figure 7.1. Representation of North Korean scheme to sell natural resources to facilitate WMD and missile commodity purchases. Credit: FinCEN, "Advisory on North Korea's Use of the International Financial System," November 2, 2017.

[1] FinCEN, "Advisory on North Korea's Use of the International Financial System," November 2, 2017.
[2] *Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System,* 2017.

The graphic shows how the front or shell companies "then use the received payments to purchase and ship commodities to the DPRK. These commodity shipments in turn may be used to smuggle goods that the North Korean government uses to build its WMD and ballistic missile programs."

Case 7.2: North Korea's Movement of Money Using the Diplomatic Pouch

The UN Panel's report from March 2018 explains how North Korea moved money from Uganda in one instance, which has a military training relationship with North Korea and allows the presence of the North Korean arms agency, KOMID. KOMID is "Pyongyang's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons…[and] has offices in multiple countries and facilitates weapons sales for the North Korean government."[3] It is supported by the Reconnaissance General Bureau. A cash smuggling scheme was reportedly uncovered following a tip from U.S. intelligence agencies. A diplomatic pouch was "carried by KOMID officials' wives about to fly out of Uganda." Uganda expelled two KOMID representatives, according to the UN Panel's March 2019 report, preventing the transfer of cash belonging to North Korea as a result of illicit business there. The Panel was unaware of what became of the cash, noting that Ugandan Ministry of Defense personnel are likely involved in the KOMID relationship and Uganda had not replied to its request for information.[4]

Case 7.3: How North Korea's Illicit Projects Abroad Raise Funds

One North Korean entity, Malaysia Korea Partners (MKP), was identified in the March 2018 Panel of Experts report as an entity that brings in millions of dollars in funds for the North Korean government by overseeing various projects in Africa, such as in Uganda, Angola, and Zambia.[5] Once detected, at least one of the North Korean operators of the Ugandan operation run by MKP changed their nationality and company holdings to Malaysian. MKP also "owns the International Consortium Bank in the North Korean capital," which ostensibly facilitates movement of money as needed.[6] The UN Panel found:

> *The [MKP] network benefits heavily from a decentralized corporate model that helps to distance the Group's activities from its beneficiaries of the Democratic People's Republic of Korea on paper and from the cooperation of non-nationals of the Democratic People's Republic of Korea, including prominent political and business figures in the countries in which they operate. Furthermore, the Panel found that several firms and, in some cases,*

[3] U.S. Department of State, "Fact Sheet: United States Sanctions Individuals Linked to North Korean Weapons of Mass Destruction Programs," March 8, 2013.
[4] *Report of the Panel of Experts*, March 5, 2019; *Report of the Panel of Experts*, August 30, 2019.
[5] Parkinson, "Never Take Their Photos."
[6] Jake Maxwell Watts, Tom Wright, and Nicholas Bariyo, "The Killing of Kim Jong Nam: Malaysia Probes Firm for North Korea Sanctions Violations," *The Wall Street Journal,* March 28, 2017.

foreign governments, have been supporting the efforts of the network to find financing for its activities, in contravention of provisions in the resolutions prohibiting such activities.[7]

MKP is made up of a consortium of 13 linked companies. One such company is Korea General Corporation for External Construction (GENCO or KOGEN), which operates in Zambia and has all North Korean directors. GENCO/KOGEN is also linked to Mansudae Overseas Project Group, which has active projects in several countries, such as Algeria, Botswana, Cambodia, Madagascar, Malaysia, and Namibia. The UN Panel wrote in its March 2019 report, "Indeed, Mansudae, MKP and GENCO/KOGEN have all, in some combination, claimed to have worked on the same projects."[8] GENCO/KOGEN activities tracked by the Panel showed that it has a significant presence in "several countries in the Middle East, Africa and Eurasia, where it uses laborers, prohibited cooperative entities and joint ventures of [the DPRK] and earns significant revenue."[9] One joint venture is with a UAE company, and other ventures were tracked to Russia, Nigeria, Cote d'Ivoire, and Equatorial Guinea. GENCO/KOGEN maintains bank accounts in Russia and has multiple joint ventures in Russian companies, including three major ones, which employ hundreds of North Korean laborers.[10] The UN Panel graphic below illustrates the connections of the KOGEN/GENCO network and its ties to MKP and Mansudae.

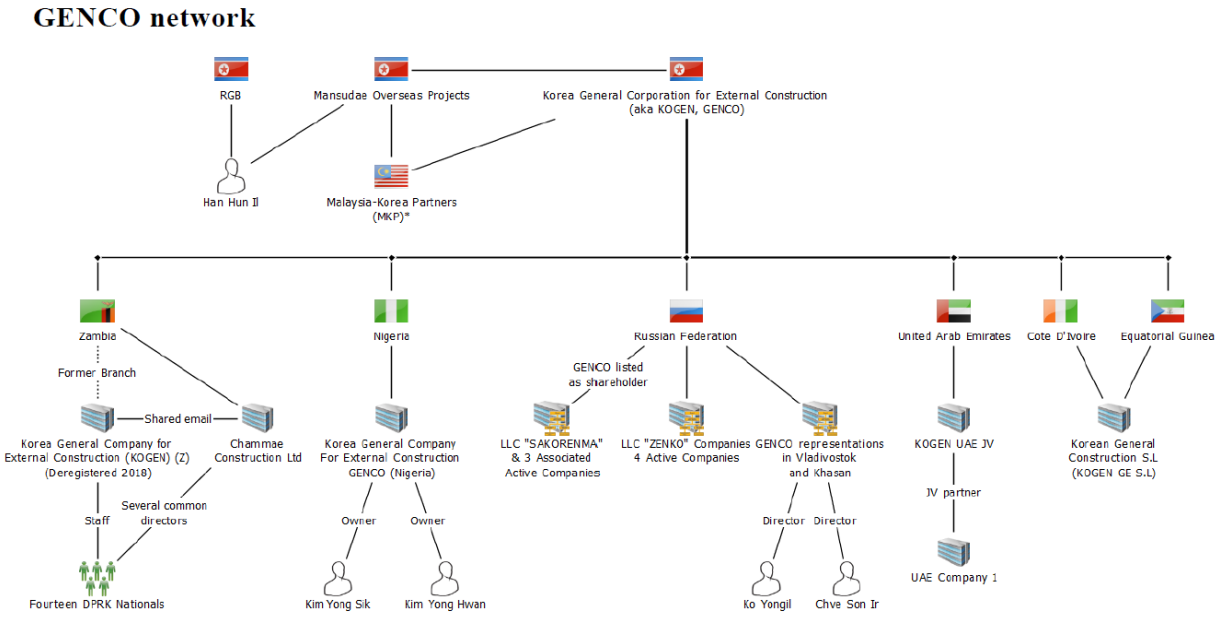


Figure 7.2. Representation of the GENCO network's activities. Credit: *Report of the Panel of Experts*, March 5, 2019.

[7] *Report of the Panel of Experts*, March 5, 2018, p. 60.
[8] *Report of the Panel of Experts*, March 5, 2019, p. 55.
[9] Ibid.
[10] Ibid, p. 56.

Case 7.4: Chinese Banks' Facilitation of North Korean Illicit Finance for Coal Exports

A U.S. District Court of Appeals case in 2019 moved to hold in contempt three Chinese banks, two with U.S. branches, that were suspected of facilitating illegal North Korean transactions. The United States had issued grand jury subpoenas for the financial records of the three banks and they refused to comply. In a partially redacted opinion, the court overruled the objections of the Chinese banks and stated, "the U.S. government has collected substantial evidence that a now-defunct Chinese company [redacted] acted as a front for [redacted], a North Korea-owned entity…by facilitating transactions that violated the sanctions orders […] The Company's assistance allegedly enabled North Korea to export hundreds of millions of dollars of coal, generating revenue in U.S. currency that North Korea could then use to requisition other commodities vital to its weapons program."[11]

The court wrote that the company would allegedly use the Chinese banks, in which the Chinese government holds a substantial minority stake, to make transactions with their banks' U.S. correspondent bank accounts. The court found the banks' arguments to be inadequate to withhold records, and the U.S. government can continue imposing daily fines until the banks comply.

Case 7.5: North Korea's Illicit Maritime Coal Exports and Coal Laundering

The UN Panel of Experts, via member states, has collected extensive records of coal transfers observed via satellite imagery, mainly in the Gulf of Tonkin, as well as rampant use of the North Korean port of Nampo to load coal, in violation of sanctions. North Korea uses re-flagged vessels, "double-flagged vessels" (rendering them stateless and more immune to inspection), ship "identity laundering" where the ship's name is concealed and the ship is re-numbered, and it turns off its automatic identification system (AIS) transponders. The Panel documented instances of illicit coal smuggling involving intermediaries in Indonesia, South Korea, and Russia.[12]

North Korea has also sold coal onward to unwitting countries after laundering its origin in Russia.[13] In mid-2017, for example, media reporting found that four North Korean ships arrived at Russia's port of Kholmsk in Chinese-owned ships that bore false Togo and Panama flags.

---

[11] United States District Court of Appeals, District of Columbia Circuit, *Opinion for the Court,* Case No. 19-5068, Filed August 6, 2019, https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rDMmQxd0Nmys/v0

[12] See Panel of Experts reports for 2018 and 2019.

[13] Guy Faulconbridge, Jonathan Saul, and Polina Nikolskaya, "Exclusive: Despite Sanctions, North Korea Exported Coal to South Korea, Japan via Russia – Intelligence Sources," Reuters. January 25, 2018, https://www.reuters.com/article/us-northkorea-missiles-coal-russia/exclusive-despite-sanctions-north-korea-exported-coal-to-south-japan-via-russia-intelligence-sources-idUSKBN1FE35N

They offloaded the coal and literally "transformed [it] into Russian coal, which can be legally sold anywhere."[14] The scheme appeared to be regularized.

Case 7.6: Chinese and Russian Entities Help North Korea Bust Financial and Nonproliferation Sanctions

On August 22, 2017, the U.S. Department of Justice announced two lawsuits against networks in China and Singapore (the latter involving Russian-owned entities and individuals) allegedly involved in financial and nonproliferation sanctions-busting. The lawsuits alleged that the rings were working to help North Korea buy or sell goods internationally and then launder the money for its nuclear, missile, and military programs. The accused allegedly violated U.S. laws when funds passed through U.S. correspondent banking accounts. The two rings cooperated on financial transaction schemes, according to legal documents.[15] The U.S. government froze millions of dollars in assets of both rings and asked for their forfeiture *in rem*.* At times, it uses civil actions to go after the financial assets of alleged lawbreakers located outside of U.S. jurisdiction. The lawsuits were announced alongside a broader set of Treasury Department sanctions against Chinese and Russian companies and individuals for their support to North Korea's industries that fund its WMD programs.[16]

Banned North Korean Coal Sales: Dandong Chengtai et al. of China

The U.S. District Court for the District of Columbia filed a civil suit against Dandong Chengtai Trading Limited of China, its aliases and associated names, and its owner, Chi Yupeng. The suit asked for the forfeiture of $4,083,935 in Dandong Chengtai assets that were frozen by the U.S. government. The U.S. Complaint arose out of a Federal Bureau of Investigation (FBI) investigation that alleged Dandong Chengtai and its aliases, such as Dandong Zhicheng, Rambo Resources, Ruizhi Resources, Shun Mao Mining, Maison Trading, and its owner Chi Yupeng, schemed to "launder U.S. dollars through the United States on behalf of sanctioned entities in

---

[14] Joby Warrick, "High Seas Shell Game: How a North Korean Shipping Ruse Makes a Mockery of Sanctions," *The Washington Post,* March 3, 2018, https://www.washingtonpost.com/world/national-security/high-seas-shell-game-how-a-north-korean-shipping-ruse-makes-a-mockery-of-sanctions/2018/03/03/3380e1ec-1cb8-11e8-b2d9-08e748f892c0_story.html?utm_term=.e5599a30cdd8

[15] United States District Court for the District of Columbia, *Complaint: United States of America vs. $4,083.935.00 of funds associated with Dandong Chengtai Trading Co., Ltd, Defendant in Rem, aliases and associated entities, and Chi Yupeng,* Case 1:17-cv-01706, Filed August 22, 2017.

* *In Rem,* as defined by the Law.com legal dictionary, means: "Against or about a thing," referring to a lawsuit or other legal action directed toward property, rather than toward a particular person. Thus, if title to property is the issue, the action is "in rem." The term is important since the location of the property determines which court has jurisdiction and enforcement of a judgment must be upon the property and does not follow a person. "In rem" is different from "in personam," which is directed toward a particular person.

[16] Carol Morello and Peter Whoriskey, "U.S. Hits Chinese and Russian Companies, Individuals with Sanctions for Doing Business with North Korea," *The Washington Post,* August 22, 2017, https://www.washingtonpost.com/world/national-security/us-sanctions-chinese-and-russian-companies-and-individuals-for-conducting-business-with-north-korea/2017/08/22/78992312-8743-11e7-961d-2f373b3977ee_story.html?utm_term=.82503b92f0d6

[North Korea] via the sale of coal."[17] According to information obtained from defectors cited in the case, coal funds were routed through North Korea's Office 39, the organization that handles illicit finance and maintains foreign currency and reserve funds for Chairman Kim Jong Un, the Worker's Party, and the military. Kim uses the funds almost entirely (the defector claimed 95 percent) to pay for North Korean nuclear, missile, and other weapons programs. The funds in this case appear to have been used by the Chinese entities to purchase other items on behalf of North Korea, including dual-use nuclear and missile components and luxury items, in order to avoid sending dollars back to North Korea. The entities and individuals named in the case are located in China, apart from Maison Trading, which is "purportedly headquartered in the Marshall Islands." More than $4 million in funds were frozen after Dandong Chengtai wired money to Maison Trading, where the funds were routed through the U.S. correspondent banking accounts.

Four alleged counts described in the Complaint were violations of the United States' International Emergency Economic Powers Act (IEEPA), North Korea Sanctions and Policy Enhancement Act (NKSPEA) of 2016, its conspiracy statute, and money laundering statute. The actions also violated UN sanctions on North Korea.

The Scheme

A FinCEN finding included in the Complaint summarizes the alleged scheme: North Korea makes "extensive use of deceptive financial practices, including the use of shell and front companies to obfuscate the true originator, beneficiary, and purpose behind its transactions," in part "to evade international sanctions."[18] In this case, the North Koreans schemed to export vast amounts of coal and other goods to Chinese entities, which then re-sold the coal and used the profits to fulfill shopping lists of items for North Korea. At times, various debts were canceled among entities as payment (use of the barter or "book-to-book" scheme). In this way, the Chinese entities were largely able to avoid paying North Korea in dollars.

The so-called Chi Yupeng Network of Companies, which includes the aliases and alternate names in the lawsuit, was responsible for importing nearly $700,000,000 worth of coal from North Korea between January 2013 and February 2017. China officially (although not covertly) suspended North Korean coal imports in February 2017.[19] Financial records cited in the Complaint reveal that the network wired out at least $60,000,000 in U.S. dollars since NKSPEA's enactment in 2016 alone. Chi Yupeng was purportedly one person trusted by Office 39 among a close cadre of reliable middlemen who exploit the international financial system on behalf of North Korea, according to a defector. The Complaint also noted that Dandong Chengtai "allegedly used the foreign exchange received from the end users of the North Korean coal to purchase other items for North Korea, including nuclear and missile components." The

[17] Ibid.
[18] Ibid, p. 9.
[19] Chen Aizhu, "Exclusive: China's CNPC Suspends Fuel Sales to North Korea as Risks Mount – Sources," Reuters. June 28, 2017, https://finance.yahoo.com/news/exclusive-chinas-cnpc-suspends-fuel-012344827.html

Complaint did not further describe these items or activity except to indicate a general scheme to move military related items into North Korea. It also listed other items sought by North Korea such as luxury items, cell phones, sugar, rubber, petroleum products, and soybean oil.

This scheme gave rise to the UN sanctions resolution in August 2017 that further restricts North Korea's ability to export coal. The Complaint states, "in particular, coal trade has generated over $1 billion in revenue per year for North Korea, activity which prompted the UN Security Council to seek to sharply curtail such exports in November 30, 2016, and then to fully ban them in August 5, 2017."[20] OFAC designated Dandong Chengtai and its aliases on August 22, 2017, along with two other Chinese coal companies. Dandong Chengtai, the largest importer of North Korean coal, has also been involved with other sanctioned entities, such as the North Korean Koryo Credit Development Bank and Korea Ocean Shipping Agency, and the Chinese telecommunications company recently fined by the United States, ZTE Corporation, along with its front companies.

Gasoil Sales to North Korea: Velmur Management and Transatlantic Partners (both partly Russian-owned) of Singapore

Also on August 22, 2017, the Department of Justice announced a civil suit by the U.S. District Court in the District of Columbia against two front companies, Velmur Management and Transatlantic Partners, of Singapore. The United States froze $6,999,925 in assets of Velmur Management, which is partly Russian-owned; Transatlantic is also partly Russian-owned. The Complaint arose out of an FBI investigation that found that Velmur and Transatlantic schemed with a Russian company, JSC Independent Petroleum Company (IPC), and a North Korean bank, the North Korean Foreign Trade Bank (FTB), to launder millions of dollars through U.S. correspondent accounts for North Korean purchases of IPC gasoil.[21] The Complaint explained that gasoil is "a distilled petroleum product such as gasoline and/or diesel fuel," and that North Korea became highly dependent on Russia gasoil imports in 2017. Other front companies were involved in the scheme, such as entities registered in Singapore and Hong Kong and/or China. At least two illicit transactions tracked by the investigation allegedly involved Dandong Chengtai of China and its aliases.. The lawsuit alleged that Velmur was involved in seven wire transfers made from FTB via Transatlantic and others, to the Russian company IPC, representing the nearly $7 million in frozen assets. FTB and IPC were sanctioned by the Treasury Department in 2013 and June 2017, respectively. The Complaint found that Velmur and Transatlantic schemed to wire at least $20 million in U.S. dollars in recent years.

The Complaint concluded, "These opaque U.S. dollar transactions by front companies promote IEEPA and NKSPEA violations, by preventing the imposition of sanctions."[22] Much like the Dandong Chengtai case, four alleged counts described in the Complaint are violations of IEEPA,

[20] Ibid, p. 14.
[21] United States District Court for the District of Columbia, *Complaint: United States of America vs. $6,999,925.00 of funds associated with Velmur Management Pte Ltd, Defendant in Rem, and Velmur Management Pte Ltd and Transatlantic Partners Pte Ltd,* Case 1:17-cv-01705-RC, Filed August 22, 2017.
[22] Ibid, p. 10.

NKSPEA, the conspiracy statute, and the money laundering statute. The actions also violated UN sanctions on North Korea.

The Scheme

The Complaint discussed the scheme by highlighting a FinCEN report on North Korea's money laundering techniques. The report found, "North Korea conducts almost no banking in true name in the formal financial system given that many of its outward facing agencies and financial institutions have been sanctioned by the United States, the United Nations, or both." However, FinCEN noted, "North Korea does have access to the U.S. financial system through a system of front companies, business arrangements, and representatives that obfuscate the true originator, beneficiary, and purpose of transactions," which has allowed North Korea to launder millions of dollars through the U.S. correspondent accounts.[23] In this case, it used those illicit partners, located in Singapore and Hong Kong and/or China, to access the U.S. financial system.

In 2013, according to the Complaint, FTB "developed and instituted an inter-bank clearing system in North Korea." After this system was put in place, North Korean banks needed to maintain currency clearing accounts at FTB, and FTB became responsible for setting currency exchange rates. This reform "in effect, channeled transactions from North Korea's arms exports and luxury goods imports through FTB."[24] OFAC noted in its 2013 designation that FTB is used "to facilitate millions of dollars in transactions on behalf of actors linked to [North Korea's] proliferation network." FTB used the front company Transatlantic and other front companies to send U.S. dollars to Velmur. Velmur then transferred the funds to IPC, the Russian petroleum products supplier. IPC would then ship gasoil to North Korea.

The Complaint noted that Velmur was registered in Singapore in 2014 and describes itself as a commercial and industrial real estate management company. A source told investigators that it is operated in part by a Russian national, Irina Huish. Huish was added to OFAC designations on August 22, 2017. Velmur "bears the hallmarks of a front company." It has no website and may not actually use its registered address. The Complaint stated that, in fact, numerous companies were registered at its address.

Transatlantic is also apparently a front company that was registered in Singapore in May 2016 and operates on behalf of North Korea's illicit financing schemes. It was added to OFAC sanctions on August 22. A source told investigators that Transatlantic is operated in part by Andrei Serbin, a Russian national who was also designated on August 22. Transatlantic reached a contract with Daesong Credit Development Bank in the past, which has been under U.S. sanction since 2016. OFAC also designated Mikhail Pisklin, a Russian national, who worked to conclude the contract between Transatlantic and Daesong Credit Development Bank. Daesong Credit Development Bank has laundered millions of dollars through the U.S. financial system.

[23] Ibid, p. 13.
[24] Ibid, p. 15.

The Complaint describes how Velmur's operator, Huish, and Serbin worked together for the gasoil deliveries to North Korea.

One of the investigation's confidential sources revealed that Transatlantic contracted with Velmur on December 6, 2016, for the purchase by Transatlantic of 5,000 metric tons of gasoil. An addendum to the contract was added on May 11, 2017.

The Complaint described three other unnamed companies that worked closely with Velmur on sending illicit payments on behalf of North Korea. The first company (Company 1) was registered in Hong Kong as of 2008 but bank records showed an address in Qingdao City, China. The second company (Company 2) was registered in Singapore in October 2016. It apparently had no actual physical office space but its address was listed as being in the same building as Transatlantic. The third company (Company 3) was registered in Singapore in May 2014; its website was registered in 2016 using an anonymization service, and it identified itself as a petrochemical company on its website but as a logistics provider and trader in corporate registry records. It did not appear to have an actual physical office space but shared a virtual office address used by many companies.

JSC Independent Petroleum Company, or IPC, was designated by OFAC in June 2017. It has contracted with North Korea for oil sales and has shipped over $1 million in petroleum products to North Korea.

The Complaint stated that in September 2016, Dandong Chengtai of China wired $230,000 to Velmur. Dandong Chengtai is also known to have made payments on behalf of FTB. In July 2016, Ruizhi Resources, one of Dandong Chengtai's front company aliases or affiliates, also wired $189,980 to Velmur.

In 2016, the Complaint stated, an FTB front company wired two payments to Velmur totaling more than $250,000. A confidential source told investigators that this front company worked for FTB and it had previously made payments to third parties for FTB.

In 2017, another FTB front company made two payments to Velmur totaling more than $500,000. The aforementioned source stated to investigators that this front company had previously made payments on behalf of FTB.

The Complaint tracked each of the seven wire transfers made from Velmur to IPC via Transatlantic and others. Another confidential source to the investigation provided a bill of lading for May 2017 shipments of diesel fuel by IPC to North Korea, departing from Port Vladivostok, Russia. The port is "a known waypoint for Russian transshipments to North Korea." Shipping data gathered by investigators showed a steady stream of oil tanker traffic between Vladivostok and North Korea at the time.

Illicit Transactions

The Complaint described how Transatlantic and other front companies wired North Korean money through Velmur. The funds described below made up portions of the assets frozen by the U.S. government.

An undated payment confirmed by a source, in the amount of $1.09 million, was made from a "clandestine FTB branch located outside North Korea" via an FTB front company, to Velmur.

On May 5, 2017, Company 1, described above, wired Velmur $1,199,975 for gasoil. Two additional payments were made. U.S. or foreign banks appear to have frozen those transactions.

Company 2, also described above, had previously wired funds to Company 1. It wired $350,000 to Company 1 on May 2, 2017. Three days later, Company 1 wired Velmur the $1,199,975 for gasoil. On May 12, after U.S. or foreign banks appear to have frozen the transactions described above, Company 2 attempted to wire Velmur a payment in the amount of $1,200,000. This transaction was apparently also frozen.

Two additional companies then attempted payments to Velmur. On May 12, Transatlantic wired $1,510,000 to Velmur for gasoil. This transaction was frozen. On May 24, Company 3 (described above) wired $500,000 to Velmur for gasoil. This transaction was apparently frozen. On June 1, Transatlantic wired $490,000 to Velmur for gasoil. This transaction was also frozen.

Case 7.7: The Glocom Network, Part of North Korea's Foreign Military Goods Sales Operations

North Korea is forbidden from engaging in military-related imports and exports under Resolution 1874 (2009). But for several years, the UN Panel of Experts on North Korea has been investigating the financial operations of Glocom (Global Communications Co.) of Malaysia, which it characterizes as "a Reconnaissance General Bureau [intelligence service]-directed network selling prohibited military communications technology."[25] It has sold military-related goods to Eritrea and Syria, the latter via KOMID representatives in Syria. It even distributes catalogues offering military technologies and holds booths at Malaysian arms exhibits. Glocom is operated "by the Pyongyang branch of a Singapore-based company called Pan Systems," per the UN Panel's March 2018 report.[26] North Korea in turn operates and owns Pan Systems, which is run by Reconnaissance General Bureau officials. In July 2016, the Panel described, an unnamed country intercepted "an air shipment of North Korean military communication equipment, sent from China and bound for Eritrea…"[27]

[25] *Report of the Panel of Experts*, March 5, 2018.
[26] James Pearson and Rozanna Latiff, "North Korea Spy Agency Runs Arms Operation out of Malaysia, U.N. Says," Reuters. February 26, 2017.
[27] Ibid.

Glocom is another off-shore North Korean entity that relies on facilitating financial transactions with a key North Korean financial institution, principally Daedong Credit Bank, basedin Pyongyang, North Korea, as well as financial institutions in other countries, such as in Europe, Hong Kong, Singapore, Malaysia, Indonesia, China, and the broader Middle East (see Figure 7.3).[28] Glocom and a key representative, Kim Chang Hyok, also a North Korean intelligence agent, control other front companies which conduct business in Malaysia and abroad, such as Golden Services and International Global System. International Global System was used to establish Glocom. According to documentation seen by the Panel of Experts, an unnamed Malaysian bank that created accounts for these entities "was fully aware that these accounts were controlled by the [DPRK]."[29] According to the Panel, Kim Chang Hyok made near daily cash withdrawals from personal Malaysian accounts in split transactions. "Periodic bulk cash injections or large in-house cheque deposits replenished the accounts." The origin of the injections or deposits was bulk cash deposits into Glocom's bank accounts in Pyongyang. The UN report continues (split into short paragraphs for ease of understanding):

> *This deposit would be reconciled by ledger with accounts controlled by Kim Chol Sam, the then-representative of the Daedong Credit Bank in China. On the same or the next day, Kim Chol Sam would initiate a transfer to the intended recipient in Malaysia or Singapore for the same amount.*
>
> *To do so, actual funds would flow from the account where the deposit had been recorded to a Democratic People's Republic of Korea controlled front company in Hong Kong, less transfer fees and a commission for middlemen. The front company would then in turn remit funds to the intended recipient.*
>
> *As a result, the receiving financial institution in Malaysia or Singapore would see only an incoming payment from the Hong Kong front company, rather than one from International Global System or Pan Systems — the actual holders of the accounts with the Daedong Credit Bank.*
>
> *The same is true of correspondent banks processing the transactions, including those in New York, which would have little insight into the origin or beneficiaries of the transaction.*
>
> *In addition to paying suppliers in this fashion, Glocom used the same method to move money within its own network, specifically between its front company accounts in Pyongyang and those in Malaysia.*[30]

Key North Korean intelligence agents were also involved.

---

[28] *Report of the Panel of Experts*, March 5, 2018; *Report of the Panel of Experts*, March 5, 2019.
[29] *Report of the Panel of Experts*, March 5, 2018, p. 64.
[30] Ibid, p. 65.

Pan Systems, the Singapore-based company, is run by a North Korean intelligence agent named Ryang Su Nyo, and Pan Systems also lists Ryang as a shareholder of International Global System. Pan Systems uses bank accounts in China and Malaysia to buy and sell components of military communications systems. Ryang was detained in Malaysia in 2014 for trying to smuggle $450,000 through customs. Malaysia did not press charges. A Reuters investigation noted that a high-level Malaysian official who is also a director of International Golden Services, with ties to Glocom, could be shielding the company from regulatory or enforcement action.[31]

The UN Panel concluded that the Glocom network shows that:

> *…Multiple overseas accounts, especially those established in the name of front companies with the assistance of trusted local partners, allowed [the network] to continuously move funds between and in different banks and jurisdictions. The network's transactions, whether for purposes of moving money between accounts it controlled in its own network or for paying suppliers, often involved an array of evasion tactics, including large-scale use of bulk cash, front companies in Hong Kong and elsewhere, middlemen and a ledger system.*

The Panel updated its investigation in its March 2019 report, stating that the operations of Glocom continue. It stated, "Unlike most front companies of the [DPRK], which tend to close and reappear with a new guise after being publicly investigated, Glocom has continued to actively use its brand despite previous Panel recommendations that Member States freeze bank accounts and other assets owned by all individuals and entities acting on behalf of Pan Systems or Glocom."[32] Moreover, "Glocom reinforced its online presence in 2018 with a website redesign and descriptions of an array of new products." It continued, "An open-source report in August 2018 linked Glocom's IP address through a second high-tech front company to [DPRK owned] restaurants…in Viet Nam. Furthermore, in mid-2018, Glocom sought to further expand its reach by forming relationships with radio technology distribution companies in Malaysia and Indonesia."

[31] "North Korea Spy Agency Runs Arms Operation out of Malaysia, U.N. Says."
[32] *Report of the Panel of Experts*, March 5, 2019, p. 57.

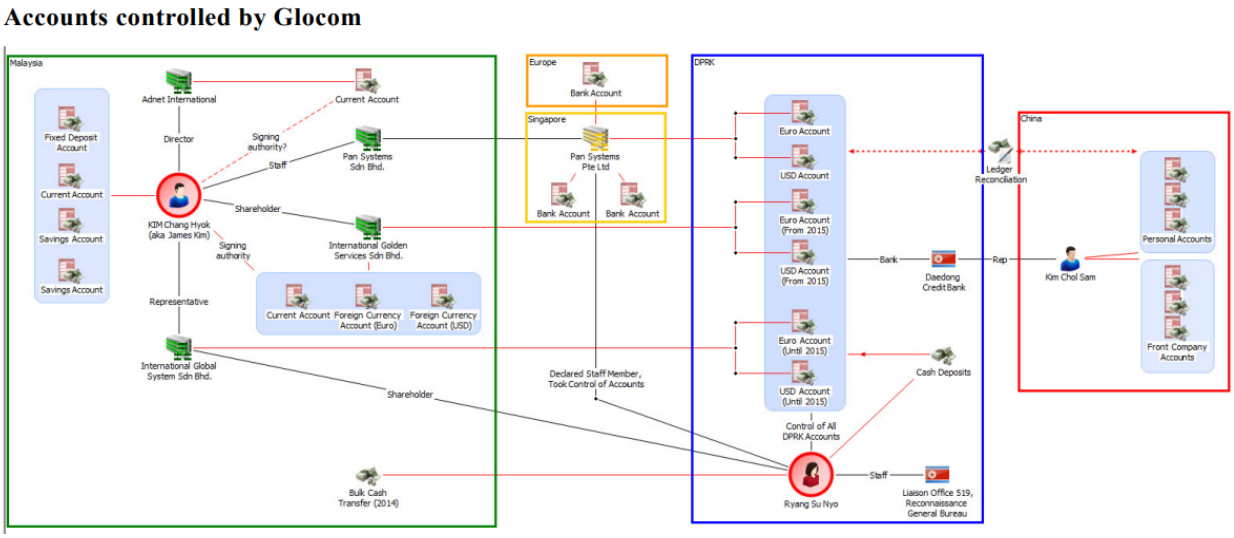


Figure 7.3. Diagram showing flow of transactions and relationships between various front companies and banks used by North Korea in the Glocom network. Credit: *Report of the Panel of Experts,* March 5, 2018, p. 64.

Case 7.8: Hong Kong-Based Front Company Alleged to Operate and Launder Millions for North Korea

On June 14, 2017, the U.S. District Court in the District of Columbia filed a civil action *in rem* against Mingzheng International Trading Limited of Hong Kong, for the forfeiture of $1,902,976 held in U.S. bank accounts.[33] The action followed an inquiry by the FBI into Mingzheng, which the FBI found to be a front company incorporated by North Korea "to launder U.S. dollars on behalf of sanctioned North Korean entities."[34] North Korea's sanctioned Foreign Trade Bank (FTB), owned by the state, is alleged to have used shell companies such as Mingzheng "to make U.S. dollar payments on behalf of a covert foreign branch of FTB, which is otherwise barred from making such U.S. dollar payments." The Complaint alleged that "between October and November 2015, Mingzheng was a counterparty to 20 illicit wire transfers in U.S. dollars through District of Columbia banks, totaling $1,902,976.00…" The transfers were allegedly violations of the IEEPA and conspiracy and federal money laundering laws.

The Scheme

According to the U.S. Complaint, the Foreign Trade Bank of North Korea "is responsible for handling foreign currency transactions for North Korea's government ministries and their subordinate trading companies." Following reforms in the mid-2000s, North Korean banks "were generally required to maintain currency clearing accounts at FTB." The reform, the Complaint states, "in effect, channeled transactions from North Korea's arms exports and

[33] United States District Court in the District of Columbia, *Complaint: United States of America v. Mingzheng International Trading Limited, various amounts of funds associated,* Case 1:17-cv-01166, Filed June 14, 2017.
[34] Ibid.

luxury goods imports through FTB."[35] The United States' Section 311 action (designation of North Korea as a primary jurisdiction of money laundering concern) found that FTB has laundered millions of dollars in violation of U.S. sanctions.

The complaint describes information from two confidential sources who informed the FBI that Mingzheng "launders U.S. dollar payments on behalf of North Korean entities – in particular, FTB."[36] The FBI found that Mingzheng lacks a website, a legitimate business purpose, and "makes U.S. dollar payments for products in totally unrelated industries," according to a search of international wires. The first source claimed that Mingzheng carried out transactions for North Korea between January 2012 and January 2015. The second source provided information "tying FTB to Mingzheng and the wiring of the Defendant Funds" such as coded reference numbers showing that Mingzheng was making U.S. dollar payments for FTB. Furthermore, the second source told the FBI that Mingzheng "acts as a front company for a covert Chinese branch of FTB. This branch is operated by a Chinese national who has historically been tied to FTB." As the UN Panel of Experts noted in its 2017 report, "Despite strengthened financial sanctions in 2016, the country's networks are adapting by using greater ingenuity in accessing formal banking channels, as well as bulk cash and gold transfers."[37]

The timeframe of the alleged 20 illicit wire transfers carried out by Mingzheng on behalf of FTB was October 19, 2015 to November 18, 2015. The FBI identified three Chinese banks that allegedly facilitated the transactions as banks where Mingzheng held accounts: China Merchants Bank (CMB), Bank of Communications (BOC), and Shanghai Pudong Development Bank (SPDB). The wire transfers allegedly violated U.S. law as they were cleared through U.S. correspondent banking accounts. In addition, these banks were allegedly involved in other North Korean illicit finance schemes involving Chinese entities and individuals under investigation, indictment, or administrative actions by the United States.

The second source told the FBI that Mingzheng payments were "being remitted to a Chinese Export and Import Company (termed "Chinese Company 1" in the Complaint) that had previous ties to Dandong Hongxiang" (Industrial Development Co. Ltd.), a sanctioned Chinese trading company known for illegal North Korea business. Four Chinese nationals working for the company were indicted by the District of New Jersey in 2016 for allegedly laundering U.S. dollars for KKBC, a sanctioned North Korean bank.[38] Documents from the Dandong Hongxiang investigation showed that Dandong Hongxiang and its front companies made U.S. dollar payments to Chinese Company 1 between 2009 and 2013, totaling $3.19 million.[39] The FBI reviewed international wire transfers which revealed that FTB likely made payments to Chinese

[35] *Complaint: United States of America v. Mingzheng International Trading Limited,* Filed June 14, 2017.
[36] Ibid, p. 13.
[37] *Report of the Panel of Experts,* February 27, 2017, p. 4.
[38] U.S. Department of Justice, "Four Chinese Nationals and China-Based Company Charged with Using Front Companies to Evade U.S. Sanctions Targeting North Korea's Nuclear Weapons and Ballistic Missile Programs," Press Release, September 26, 2016, https://www.justice.gov/opa/pr/four-chinese-nationals-and-china-based-company-charged-using-front-companies-evade-us
[39] *Complaint: United States of America v. Mingzheng International Trading Limited,* Filed June 14, 2017.

Company 1 between 2012 and 2016. The second confidential source told the FBI that Mingzheng's payments to Chinese Company 1 during that timeframe were carried out on behalf of FTB, totaling $1.8 million from March 2013 to September 2014.

One Chinese national who was indicted in the Dandong Hongxiang/KKBC scheme and who was apparently involved in the Mingzheng case was Luo Chuanxu. The FBI found that, in 2015, Luo "facilitated numerous payments to Mingzheng" using one of his alleged Dandong Hongxiang front companies in Anguilla. Luo had allegedly established other front companies in the British Virgin Islands and Hong Kong. China Merchants Bank was involved in one of two alleged transfers. Another Chinese national indicted in the Dandong Hongxiang/KKBC scheme was Hong Jinhua, the deputy general manager of Dandong Hongxiang. In 2015, one Hong Kong-based front company allegedly established by Hong wired money to Mingzheng's bank account at the Bank of Communications in China. The FBI also found evidence of Dandong Hongxiang and Mingzheng having three of the same front company beneficiaries and remitters and Dandong Hongxiang made financial transactions with seven of 14 companies that Mingzheng was alleged to have transacted with.

In addition, the FBI determined that Mingzheng was "linked to a series of financial transactions with the Chinese telecommunication company ZTE Corporation (ZTE), which pled guilty to U.S. sanction violations in March 2017." One of ZTE's alleged trading companies, with ties to North Korea's Posts and Telecommunications Company (KPTC), was Chinese Company 2, another unnamed Chinese entity in the Mingzheng complaint. The complaint stated that "Mingzheng wired Chinese Company 2 approximately $2,295,728, while Chinese Company 2 was laundering funds on behalf of the North Korean government to ZTE." Mingzheng's bank account at Shanghai Pudong Development Bank was referenced in FTB wire transfer instructions. Mingzheng also received confirmation of payments to or from FTB involving Mingzheng's account at China Merchants Bank. The complaint stated, "Mingzheng's payments to ZTE further demonstrate Mingzheng's role as a major front company procuring products in U.S. dollars on behalf of North Korean entities. These U.S. dollar payments, which cleared through U.S. correspondent banking accounts, violated U.S. law, because Mingzheng was surreptitiously making them on behalf of FTB, whose designation precluded transactions."

Case 7.9: North Korean Cyber-Hacking Schemes Withdraw Millions in Cash from ATMs

In 2019, the UN Panel of Experts reported on how North Korea's Lazarus Group took over a network of ATMs to loot cash, a feat that a former Panel member stated "force[d] 10,000 cash distributions to individuals across more than 20 countries in 5 hours, suggesting the cooperation of large numbers of people on the ground."[40]

[40] "38North Interview with Stephanie Kleine-Ahlbrandt on the UN Panel of Experts Latest Report to the Security Council Published Today," *38North,* September 5, 2019, https://www.38north.org/2019/09/skleineahlbrandt090519/?utm_source=Stimson+Center&utm_campaign=2e98

The United States advised in 2018 about a North Korean ATM hacking scheme called FASTCash that had been targeting banks in Africa and Asia since 2016.[41] The U.S. government calls all North Korean malicious cyber activity "HIDDEN COBRA." In an alert in 2018, the Department of Homeland Security stated, "In one incident in 2017, HIDDEN COBRA actors enabled cash to be simultaneously withdrawn from ATMs located in over 30 different countries. In another incident in 2018, HIDDEN COBRA actors enabled cash to be simultaneously withdrawn from ATMs in 23 different countries."[42] After the computer security firm Symantec investigated the malware,[43] the U.S. government updated its alert including information on how the malware attack "remotely compromise[d] payment switch application servers within banks to facilitate fraudulent transactions." The figure shows how the attack functioned.

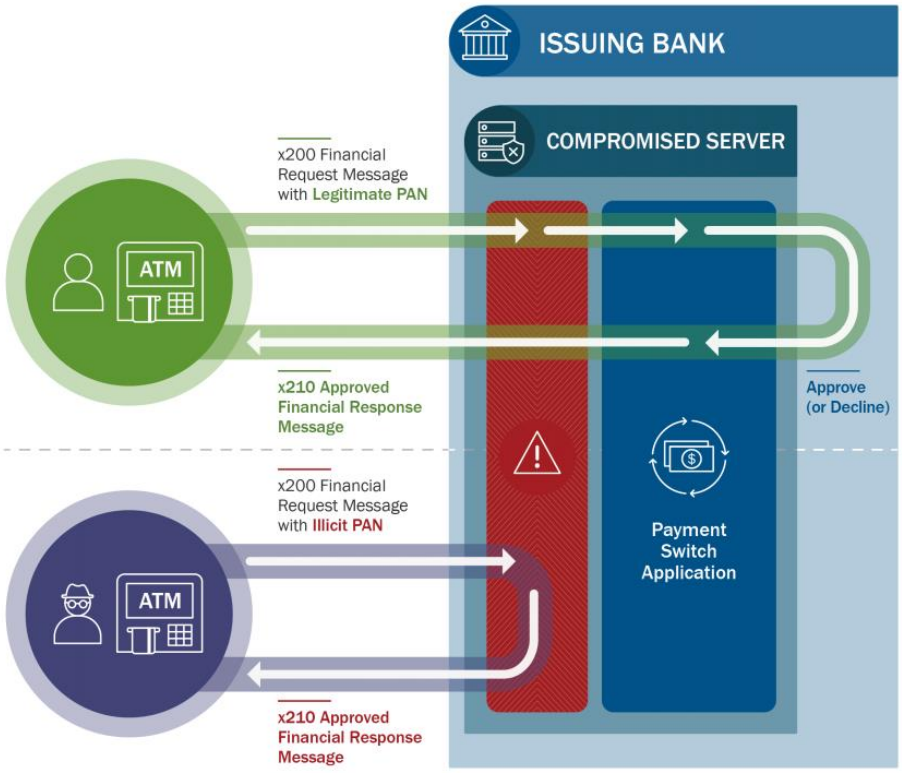


Figure 7.4. Malware attack on bank ATM systems to allow the unauthorized dispensing of cash. Credit: Symantec, "FASTCash: How the Lazarus Group is Emptying Millions from ATMs," November 8, 2018, https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

d28c83-38NDigest%2FEast+Asia%2F38+North+Digest_0901&utm_medium=email&utm_term=0_15c3e20f70-2e98d28c83-46296593&mc_cid=2e98d28c83&mc_eid=76a39e2d5e

[41] Department of Homeland Security, National Cyber Awareness System, "HIDDEN COBRA – FASTCash Campaign," October 2, 2018, Revised December 21, 2018, https://www.us-cert.gov/ncas/alerts/TA18-275A

[42] "HIDDEN COBRA – FASTCash Campaign," Revised December 21, 2018.

[43] Symantec, "FASTCash: How the Lazarus Group is Emptying Millions from ATMs," November 8, 2018, https://www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware

Section III. Shipping

Chapter 8. Introduction to International Controls for Preventing Illicit Shipping

If an illicit network succeeds in procuring a commodity from a supplier, it must next ship the item to the desired end destination. Detecting and stopping an illicitly-procured commodity already on its way from the supplier state to the proliferant state is far more difficult than detection at the procurement stage. The sheer quantity of parcel and cargo moving around the world each day via sea, land, and air presents a vast challenge for those who want to stop illicit procurements. Illicit networks use a variety, and often a combination, of deception tactics and methods to conceal the contents and ultimate consignee of packages, including misstating information on shipping labels, undervaluing contents so that the value appears to fall below reporting requirements, removing invoices characterizing the nature of goods, and shipping items through multiple countries before they reach the proliferant state. Even if a prohibited shipment is stopped at a border, customs agents may not recognize the parcel's nature without intelligence from another source. This challenge highlights the need for trained customs officials able to identify a controlled item or contact experts in their own or allied governments ("technical reachback") and flag the item for greater scrutiny or seizure.

Because of such a massive volume of shipments via sea and air, authorities and the private sector have increasingly adopted risk-based approaches for inspecting parcels or cargos going to certain countries or common transshipment points. These approaches make use of intelligence sharing and government outreach, including tips, and awareness of red flags or warning signs.

To what extent carriers, shippers, border control agents, and customs are authorized or required to act upon their suspicions depends on the domestic laws. This includes whether customs, or another agency, even have a mandate to search for and stop illicit trade, for example, beyond collecting tariffs and detecting counterfeit smuggling. However, if enabled by their government, they can form a strong line of defense in the effort to prevent proliferation-sensitive trade.

This section first provides background on international treaties, United Nations Security Council resolutions, and initiatives regulating the shipment of sensitive goods. Next, a series of case studies is considered which shows that illicit procurement networks worry about customs seizures and shipping entity interference, plan shipping-related sanctions evasions meticulously, and overall, go to great lengths to conceal illicit shipments. An annex discusses the individual parties or "stakeholders" involved in shipping (see sidebar) and their role in countering proliferation. Chapter 11 in the next section and Volume 2 provide insight into one particular network's illicit shipping practices as part of a more comprehensive study of this network's role in outfitting Iran's clandestine centrifuge program. Chapter 13 includes a summary of common methods of illicit shipping and their warning signs.

Definitions and Stakeholders

For the purpose of this section, the terms "shipping" or "shipment" cover transit, transshipment, transport, and transfer, by sea, land, and air, inland and across borders. Further, **transit** is defined as a good **passing through** a country without being off-loaded; **transshipment** is defined as a good being **off-loaded in a country and then shipped onward** in a separate shipping arrangement, changing its original route or destination to go onward to a proliferant state or another intermediary; **transport** connotes the physical **carrying** of a good; and **transfer** designates a **change in ownership** of the good. The international conventions and resolutions cited in this section may define the terms differently.

Stakeholders include customs and other border security personnel, transportation vehicle owners (such as ship, aircraft, truck, or train owners), operators (such as captains and pilots), managers, brokers, registries, shipping companies, freight forwarders, classification service providers, insurance companies, sea and airport operators, crews, industry associations, manning companies, and loan providers, such as banks. More information about the stakeholders or major actors are in the annex to this section.

International Measures to Prevent Illicit Shipment of Strategic Commodities

International laws and measures to prevent, detect, and seize strategic or proliferation-sensitive goods, in transit or during transshipment, are relatively scarce. There are a limited number of international laws, treaties, and initiatives empowering states to act to stop illicit activities and crimes via shipment by sea, land, and air. Several key UN resolutions also direct countries to implement shipping controls against the spread of sensitive goods, and periodically, the Security Council mandates countries to enforce embargoes on certain commodity shipments to specific countries. Together, these make up a loose regime of global laws for preventing illicit trade in proliferation-sensitive commodities.

The most specific resolution directed at preventing illicit transit, transshipment, and transport of proliferation-sensitive goods is UN Resolution 1540 (2004). Under two key provisions, paragraph 3 (c) and (d) (bolded below), the resolution mandated conditions relevant to shipping:

> *States shall take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials and to this end shall:*
>
> *(a) Develop and maintain appropriate effective measures to account for and secure such items in production, use, storage or transport;*

(b) Develop and maintain appropriate effective physical protection measures;

(c) Develop and maintain appropriate effective border controls and law enforcement efforts to detect, deter, prevent and combat, including through international cooperation when necessary, the illicit trafficking and brokering *in such items in accordance with their national legal authorities and legislation and consistent with international law;*

(d) Establish, develop, review and maintain appropriate effective national export and trans-shipment controls...including appropriate laws and regulations to control export, transit, trans-shipment and re-export *and controls on providing funds and services related to such export and trans-shipment such as financing, and* ***transporting*** *that would contribute to proliferation, as well as establishing end-user controls; and establishing and enforcing appropriate criminal or civil penalties for violations of such export control laws and regulations…*[1]

Of five additional implementing resolutions passed by the Security Council in support of Resolution 1540, four reiterated the need for intensified efforts by the 1540 Committee to promote full implementation of border, export, or transshipment controls.[2] Additional UN resolutions with measures against shipping banned goods, relating specifically to proliferant states such as Iran and North Korea, are described below.

The Treaty on the Non-Proliferation of Nuclear Weapons (NPT) of 1968, Chemical Weapons Convention (CWC) of 1992, and Biological Weapons Convention (BWC) of 1972 carry provisions against transfer or assistance in developing these weapons of mass destruction, and prohibitions on transit of such weapons and the commodities that lead to their construction.[3] In support of preventing nuclear transfer to non-state actors or to additional states, the Convention for the Suppression of Acts of Nuclear Terrorism and Convention on the Physical Protection of Nuclear Material (CPPNM) also prohibit nuclear proliferation-sensitive transfers.

The responsibility to control export of proliferation-sensitive goods is enhanced through state memberships in export control regimes such as the Nuclear Suppliers Group (NSG), Australia Group (AG) relating to biological and chemical weapons and their precursors, Missile Technology Control Regime (MTCR), Wassenaar Arrangement on transfer of dual-use

---

[1] *United Nations Security Council Resolution 1540 (2004),* April 28, 2004, https://undocs.org/S/RES/1540(2004)
[2] 1540 Committee, "Security Council Resolutions," https://www.un.org/en/sc/1540/resolutions-committee-reports-and-SC-briefings/security-council-resolutions.shtml
[3] *Treaty on the Non-Proliferation of Nuclear Weapons*, 1968, https://www.un.org/disarmament/wmd/nuclear/npt/text ; *Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, 1972, https://fas.org/nuke/control/bwc/text/bwc.htm ; *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction,* 1992, https://www.opcw.org/sites/default/files/documents/CWC/CWC_en.pdf

technologies and munitions, and the Arms Trade Treaty (ATT). These regimes empower states to incorporate strong measures against strategic commodity trafficking into their national laws, and to seize illicit shipments passing through their territories. Those regimes can also serve as a basis for extra-territorial seizure, such as interdicting shipments on the high seas, although jurisdiction at sea is not straightforward, as explained below.

Illicit Shipment by Sea

According to the International Maritime Organization (IMO), a specialized agency of the United Nations, international movement of goods by ship accounts for 80 percent of global trade, making seaborne shipment of controlled or sensitive goods a prime area of attention for efforts to prevent strategic commodity trafficking.[4] A number of issues arise in implementing national and international trade controls at sea, particularly on the high seas, where states frequently lack clear territorial jurisdiction and confrontation can be risky. To help clarify jurisdiction, the United Nations Convention on Law of the Sea (UNCLOS), which opened for signature in 1982 and entered into force in 1994, "la[id] down a comprehensive regime of law and order in the world's oceans and seas establishing rules governing all uses of the oceans and their resources."[5] To date, 168 nations, territories, and entities have ratified or acceded to the convention, rendering it fairly comprehensive in membership.[6] In addition to setting out an international order for territorial integrity, free navigation, transit passage, and access, as well as conduct and rules of maritime use, UNCLOS contains clauses that could allow the interception of unlawful shipments of proliferation-sensitive commodities. However, UNCLOS is not specific in covering proliferation-sensitive goods under the authorities.

According to UNCLOS Article 3, a state's territorial sea can have a breadth of up to 12 nautical miles. However, the right to control the sea under certain conditions reaches further. Article 33 says that coastal states have the right to control the sea extending 24 nautical miles from their coast, called "contiguous zone," in order to:

> *(a) prevent infringement of its customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea;*
> *(b) punish infringement of the above laws and regulations committed within its territory or territorial sea.*[7]

[4] International Maritime Organization, "Introduction to IMO," http://www.imo.org/en/About/Pages/Default.aspx
[5] *United Nations Convention on the Law of the Sea of 10 December 1982,* Overview and Full Text, https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm
[6] *United Nations Convention on the Law of the Sea,* "Table A recapitulating the status of the Convention and of the Related Agreements," updated June 27, 2019, https://www.un.org/depts/los/reference_files/status2019.pdf
[7] *United Nations Convention on the Law of the Sea of 10 December 1982,* https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Further, regarding rights of protection of the coastal state, Article 25 states:

> *1. The coastal State may take the necessary steps in its territorial sea to prevent passage which is not innocent.*
> *2. In the case of ships proceeding to internal waters or a call at a port facility outside internal waters, the coastal State also has the right to take the necessary steps to prevent any breach of the conditions to which admission of those ships to internal waters or such a call is subject*.[8]

Article 27 of UNCLOS provides for the boarding of ships within the territorial zone if criminal conduct is believed to be occurring, but under certain conditions:

> *The criminal jurisdiction of the coastal State should not be exercised on board a foreign ship passing through the territorial sea to arrest any person or to conduct any investigation in connection with any crime committed on board the ship during its passage, save only in the following cases:*
>
> *(a) if the consequences of the crime extend to the coastal State;*
> *(b) if the crime is of a kind to disturb the peace of the country or the good order of the territorial sea;*
> *(c) if the assistance of the local authorities has been requested by the master of the ship or by a diplomatic agent or consular officer of the flag State; or*
> *(d) if such measures are necessary for the suppression of illicit traffic in narcotic drugs or psychotropic substances.*[9]

A great deal of authority therefore rests with the coastal state if a ship within its territorial waters or contiguous zone is believed to be transporting illicit goods. Under Article 111, the coastal state is also given the right to carry out "hot pursuit" of a ship that has passed through its territorial waters and is suspected of breaking its laws, and that pursuit can continue to the high seas, provided that it has not been interrupted.

On the high seas, UNCLOS stipulates the right of free passage and peaceful purposes, including strong emphasis on non-interference. However, authority is given to the flag state of ships to regulate activities of ships in their registry. Under Article 91, ships must bear the flag of the state in which they are registered, and possess documents regarding their authorization, in order to fly the flag. Article 92 states, "Ships shall sail under the flag of one State only and, save in exceptional cases expressly provided for in international treaties or in this Convention, shall be subject to its exclusive jurisdiction on the high seas." Despite bearing a particular country's flag, if the country operates an open registry, the ship may be owned and operated by a different country or a variety of nationals. Despite this, under Article 94, the flag state is given authorities over activities of the ship.

[8] Ibid.
[9] Ibid.

It must:

> *(a) maintain a register of ships containing the names and particulars of ships flying its flag, except those which are excluded from generally accepted international regulations on account of their small size; and*
> *(b) assume jurisdiction under its internal law over each ship flying its flag and its master, officers and crew in respect of administrative, technical and social matters concerning the ship.*

The flag state must also ensure the physical integrity of ships, maintenance of communication systems, labor conditions, basic seafaring capabilities of the crew, and their knowledge of safety and international regulations at sea. Today, lapses in flag states exercising this authority have become more prevalent in observed cases of maritime illicit trade. An open registry (as opposed to a closed one allowing only nationally-owned ships to register) is a valuable income source for many countries, especially small island states, but frequently leads to little oversight and regulation (which is often the reason a ship-owner uses a foreign registry in the first place). From cases involving North Korea to Iran, commonly used flag states have increasingly stated little knowledge of nefarious activities of their registered ships. In allowing easy, often online, registration of ships and the right to fly their flag, and without exercising adequate diligence, they have been implicated in egregious illicit procurement and shipment schemes. This trend will be explained in more detail under specific cases involving Iran and North Korea.

Several public, though often subscription-based databases, track global vessel ownership, registration, and movement using ships' Automatic Identification Systems (AIS), or systems aboard ships that emit signals and broadcast their locations.[10] These databases clearly show how open flag registries lead to large quantities of registered ships that are often registered to small countries. For example, searching the MarineTraffic database for cargo vessels and tankers registered in Panama returned 8,636 results, while searching for those registered in the United States returned only 697 results.[11] A small state is unlikely to be able to deploy the resources necessary to regulate and oversee the activities of such a vast quantity of ships.

UNCLOS does not specify a right to board a ship on the high seas except under special circumstances. Article 110 on Right to Visit specifies boarding of a foreign ship only if it is suspected of being engaged in specific acts such as: piracy, slave trade, unauthorized broadcasting and under the jurisdiction of the flag state, sailing as a ship without nationality, or flying a false flag. Government ships involved in non-commercial service are given complete immunity except by their flag state. Article 92 also states, "A ship may not change its flag during a voyage or while in a port of call, save in the case of a real transfer of ownership or change of registry;" however, ships engaging in illicit shipping are frequently detected changing their flag status to false or convenient flags as needed. They also sail without any flag at all.

[10] Examples include: Fleetmon, MarineTraffic, IHS Maritime, VesselFinder, Windward, Eqasis, VesselsValue, VesselTracking.net, Equasis.org, and Refinitiv Eikon.
[11] Search performed on July 26, 2019.

In addition to UNCLOS, the IMO sets global standards "for the safety, security and environmental performance of international shipping." It seeks to create and implement a universal framework toward these goals. Signatories to the convention agree to implement supplementary conventions relating to such areas as maritime safety, pollution, training, liability, prevention of collisions, and, most relevant to illicit shipping, unlawful acts involving shipping. To date, the IMO has 174 member states, but state parties separately ratify the supplementary conventions.[12]

Unlawful shipping of proliferation-sensitive commodities is addressed in a 2005 Protocol to the IMO's Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention). However, while the SUA Convention entered into force in 1992 and has 156 members, the ratification of the SUA Convention's 2005 Protocol remains underwhelming. The protocol prohibits the (witting) illicit transport of radioactive material; biological, chemical, or nuclear weapons (termed "BCN" in the Convention); source material; special fissionable material; or equipment or material designed or prepared for the latter's processing, "knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an IAEA [International Atomic Energy Agency] comprehensive safeguards agreement;" and any "equipment, materials or software or related technology that significantly contributes to the design, manufacture or delivery of a BCN weapon, with the intention that it will be used for such purpose."[13] The specificity of the SUA Convention's 2005 Protocol adds another element to this loose global regime of controlling the illicit shipment of strategic commodities. After almost five years, the Protocol now has the required number of ratifications needed to enter into force, with 48 contracting states.[14]

The SUA Convention's 2005 Protocol, Article 8, also lays out procedures and guidelines for boarding ships on the high seas that are suspected of being engaged in the aforementioned activities. A detaining ship must first request and secure permission to board from the flag state of the suspect ship. As an alternative, the "master" of the ship, acting on behalf of its owner, whether or not also the flag state, may permit detainment or inspection. The detaining ship can also seize or "detain the ship, cargo, or persons pending receipt of disposition instructions from the flag State." The parties are urged to avoid use of force. Underscoring the potential for conflict on the high seas, states are also urged to "take into account the dangers and difficulties involved in boarding a ship at sea and searching its cargo, and give consideration to whether other appropriate measures agreed between the States concerned could be more safely taken in the next port of call or elsewhere."

As mentioned above, the Automatic Identification System is one key tool for assisting the goal of detecting and preventing illicit shipping by sea is mandatory identity and location tracking for

[12] IMO, "Member States, IGOs and NGOs," http://www.imo.org/en/About/Membership/Pages/Default.aspx
[13] *Convention for the Suppression of Unlawful Acts of Violence against the Safety of Maritime Navigation,* 1988; *Protocol of 2005*, http://oceansbeyondpiracy.org/sites/default/files/SUA_Convention_and_Protocol.pdf
[14] IMO, "Status of IMO Treaties," August 5, 2019, http://www.imo.org/en/About/Conventions/StatusOfConventions/Documents/Status%20-%202019.pdf

ships. To institute the mandatory tracking of ships, the IMO's Convention for the Safety of Life at Sea (SOLAS), developed in the wake of the Titanic disaster in 1912, the most recent version which entered into force in 1980, requires ships to carry AIS.[15] AIS "are designed to be capable of providing information about the ship to other ships and to coastal authorities automatically."[16] Paragraph 2.4 states: "All ships of 300 gross tonnage and upwards engaged on international voyages and cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size shall be fitted with an automatic identification system…" The SOLAS Convention states further that AIS must: "Provide automatically to appropriately equipped shore stations, other ships and aircraft information, including the ship's identity, type, position, course, speed, navigational status and other safety-related information;…Monitor and track ships; [and]…Exchange data with shore-based facilities…" Furthermore, "Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information."[17] The AIS provisions went into effect in 2004.

Tracking AIS signals enables coastal and flag states to better ascertain the location and activities of ships passing through their territories or of those under their jurisdiction. However, as cases involving Iran and North Korea show, these ships frequently turn off their AIS transponders in order to hide their locations and illicit activities, as well as undertake a variety of other concealment methods, explained further below.

Illicit Shipment by Air

While shipment by sea is more common, shipment by air is often used for time-sensitive and valuable commodities, including goods such as "high-value machine parts and manufacturing equipment, electronic components for manufactured goods […] unique scientific instruments, [and] highly specialized tools and equipment."[18] These descriptions fit many proliferation-sensitive items, and thus air shipments must also be monitored to prevent illicit shipment of strategic goods.

There are many parallels between international maritime and aviation regulations. A state's airspace in UNCLOS is defined as the air above the state's soil and its territorial sea.[19] The IMO-equivalent for aviation is the International Civil Aviation Organization (ICAO), and similarly to commercial vessels, all commercial aircraft must be registered to a country.

---

[15] IMO," International Convention for the Safety of Life at Sea (SOLAS), 1974," http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

[16] IMO, "AIS transponders," http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx

[17] *International Convention for the Safety of Life at Sea,* 1974, http://www.mar.ist.utl.pt/mventura/Projecto-Navios-I/IMO-Conventions%20(copies)/SOLAS.pdf

[18] Bart Elias, *Security of Air Cargo Shipments, Operations, and Facilities* (Washington, D.C.: Congressional Research Service, January 24, 2018), https://fas.org/sgp/crs/homesec/R45082.pdf

[19] See part II, Article 2 in *United Nations Convention on the Law of the Sea of 10 December 1982,* https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

One relevant convention is a relatively new one, titled Convention of the Suppression of Unlawful Acts Relating to International Civil Aviation (also called Beijing Convention), opened for signature in September 2010. It entered into force in July 2018, taking almost eight years to gather the 22 ratifications needed.[20]

Article 1 of the Beijing Convention now criminalizes intentionally releasing or discharging from, or using onboard or against an aircraft, "any BCN weapon or explosive, radioactive, or similar substances."

Further, most relevant to preventing illicit trade in proliferation-sensitive goods, the convention stipulates that a person commits an offense if the person intentionally:

> *(i) transports, causes to be transported, or facilitates the transport of, on board an aircraft:*
>
> > *(1) any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, with or without a condition, as is provided for under national law, death or serious injury or damage for the purpose of intimidating a population, or compelling a government or an international organization to do or to abstain from doing any act; or*
> >
> > *(2) any BCN weapon, knowing it to be a BCN weapon as defined in Article 2; or*
> >
> > *(3) any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to a safeguards agreement with the International Atomic Energy Agency; or*
> >
> > *(4) any equipment, materials or software or related technology that significantly contributes to the design, manufacture or delivery of a BCN weapon without lawful authorization and with the intention that it will be used for such purpose;*

Much of the language is analogous to that in the SUA Convention's 2005 Protocol. Notably, the Beijing Convention makes anyone *intentionally* involved in illicit transport of proliferation-sensitive goods using civil aircraft liable for the act, much like the SUA Convention with regard to ships. It makes no exception for ship operator, crew, airline, or airline staff. Since war aircraft and government aircraft are not covered by the convention, they could be exploited to illicitly move goods. In determining guilt, the responsibility appears to lie with the state claiming an offense to prove the illegality, intent, and significance of any violation. Both the

[20] ICAO, "Current lists of parties to multilateral air law treaties," accessed August 1, 2019, https://www.icao.int/secretariat/legal/Lists/Current%20lists%20of%20parties/AllItems.aspx

SUA Convention and the Beijing Convention stipulate steps to be taken upon detecting a violation, including, if the offender is not extradited, taking the offender or alleged offender into custody and submitting the case for prosecution. Differing from the SUA Protocol, the Beijing Convention includes no searching or boarding provisions.

In practical terms, it is difficult for countries to force an aircraft to land and then demand boarding and seizure rights, particularly if they are operating over international airspace. Searching, screening, and boarding provisions appear to depend mostly on domestic laws regulating air traffic over their airspace, with the exception of aircraft coming from and going to North Korea, for which overflying a UN member state's territory is prohibited, and screening and searching is required by UN resolutions. Another initiative developed by the United States, the Proliferation Security Initiative (PSI), explained further below, has attempted to close detainment, boarding, and seizure loopholes.

Since June 2018, in a useful move, the United States has required all airlines flying to or transiting through its airspace to use Air Cargo Advance Screening (ACAS) systems and submit cargo data to U.S. Customs and Border Protection (CBP) "at the earliest point practicable and prior to loading the cargo onto aircraft destined to or transiting through the United States."[21] This screening is motivated by the desire to prevent terrorist attacks and is focused on preventing the "loading of high-risk air cargo that could pose a risk to the aircraft during flight."[22] It also incorporates steps that may help CBP identify otherwise suspicious cargo, since its requirements include specific cargo description and shipper and consignee information.

Illicit Shipment by Land

There is no IMO or ICAO-equivalent for road or railway transit or traffic, which led one of the principal UN organs, the United Nations Economic and Social Council, and its regional commissions, to assume responsibility. Chapter 11 of the *Status of Treaties* in the United Nations Treaty Collection is titled "Transport and Communications," and lists under five sub-categories all UN conventions, protocols, amendments, and regulations regarding (a) customs matters, (b) road traffic, (c) transport by rail, (d) water transport, and (d) multimodal transport.

One of the oldest conventions, the 1956 Convention on the Contract for the International Carriage of Goods by Road, makes the carriage of a consignment note, the "CMR," (the French acronym for Carriage of Goods by Road) mandatory for all commercial transit by road. The CMR is prepared by the sender, signed by the sender and the carrier, and should contain a range of items including names and addresses of shipper and receiver, and descriptions of the goods. The CMR-equivalent for rail transport is the "CIM" (the French acronym for Carriage of Goods by Rail).

---

[21] U.S. Customs and Border Protection, "Air Cargo Advance Screening (ACAS)," https://www.cbp.gov/border-security/ports-entry/cargo-security/acas

[22] U.S. Customs and Border Protection, Fact Sheet, "Air Cargo Advance Screening (ACAS)," June 2018, https://www.cbp.gov/sites/default/files/assets/documents/2018-Jun/ACAS%20Fact%20Sheet%20060518A%20FINAL.pdf

Overall, there are few international legal mechanisms which specifically regulate trade by land, because states are generally empowered to regulate trade, including the movement of foreign goods, passing through their jurisdictions and territories. Likewise, memberships in export control regimes can be incorporated into domestic laws, and domestic laws made even more specific to the state's desires.

However, if a state is lacking national transit controls, one measure worth noting is the Convention on Transit Trade of Land-locked States, which entered into force in 1967, and ensures free access to the sea by land-locked states for the purposes of trade.[23] The convention contains a provision under Article 11 that includes exceptions to free transit "for goods of a kind which the importation is prohibited, either on grounds of public morals, public health or security…," and perhaps more ambiguously, "export or import or transit of particular kinds of articles such as narcotics, or dangerous drugs, or arms…"[24] This enables states to regulate foreign trade transiting through their territories to and from the sea.

Of note, UNCLOS has similar provisions regulating access to the sea by land-locked states, and with 168 parties, compared to 43 parties to the Convention on Transit Trade for Land-locked states, the former has practically superseded the latter.

Attempting to Fill the Gaps

An innovative initiative developed by the United States in 2003 to empower states to conduct interdictions on the high seas, by land, and by air is the Proliferation Security Initiative, or PSI. The PSI "strives to co-ordinate participating states' efforts, consistent with national legal authorities and relevant international law (e. g. UNSCR 1540) and frameworks, to stop proliferation related trade in WMDs, related materials and delivery systems."[25] It has 107 participants to date and entails endorsing a set of Interdiction Principles and participating in voluntary exercises, such as in the Mediterranean and various locations in the Asia-Pacific, during which state authorities train to interdict proliferation-sensitive shipments.[26] States commit to coordinate with other states and prioritize interdiction. They also commit to incorporate these measures into their national legal authorities. A full set of actions states commit to include:

---

[23] Status of participation to *United Nations Convention on Transit Trade of Land-Locked States,* https://treaties.un.org/PAGES/ViewDetails.aspx?src=TREATY&mtdsg_no=X-3&chapter=10&clang=_en

[24] *United Nations Convention on Transit Trade of Land-Locked States,* July 8, 1965, https://www.jus.uio.no/english/services/library/treaties/09/9-04/land-locked-states.xml

[25] Proliferation Security Initiative, "Who We Are," https://www.psi-online.info/psi-info-en/-/2075520 ; For a fuller discussion of the U.S. government administrative process involved in establishing the PSI, see: Susan J. Koch, "Proliferation Security Initiative: Origins and Evolution," Occasional Paper 9 (Washington, D.C.: National Defense University Press, Center for the Study of Weapons of Mass Destruction, June 2012), https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Occasional%20Papers/09_Proliferation%20Security%20Initiative.pdf

[26] Proliferation Security Initiative, "Endorsing States List," updated April, 2, 2019, https://www.psi-online.info/psi-info-en/botschaft/-/2205942

1) Not to transport or assist in the transport of any such cargoes to or from states or non-state actors of proliferation concern, and not to allow any persons subject to their jurisdiction to do so.

(2) At their own initiative, or at the request and good cause shown by another state, to take action to board and search any vessel flying their flag in their internal waters or territorial seas, or areas beyond the territorial seas of any other state, that is reasonably suspected of transporting such cargoes to or from states or non-state actors of proliferation concern, and to seize such cargoes that are identified.

(3) To seriously consider providing consent under the appropriate circumstances to the boarding and searching of its own flag vessels by other states, and to the seizure of such WMD-related cargoes in such vessels that may be identified by such states.

(4) To take appropriate actions to (1) stop and/or search in their internal waters, territorial seas, or contiguous zones (when declared) vessels that are reasonably suspected of carrying such cargoes to or from states or non-state actors of proliferation concern and to seize such cargoes that are identified; and (2) to enforce conditions on vessels entering or leaving their ports, internal waters or territorial seas that are reasonably suspected of carrying such cargoes, such as requiring that such vessels be subject to boarding, search, and seizure of such cargoes prior to entry.

(5) At their own initiative or upon the request and good cause shown by another state, to (a) require aircraft that are reasonably suspected of carrying such cargoes to or from states or non-state actors of proliferation concern and that are transiting their airspace to land for inspection and seize any such cargoes that are identified; and/or (b) deny aircraft reasonably suspected of carrying such cargoes transit rights through their airspace in advance of such flights.

(6) If their ports, airfields, or other facilities are used as transshipment points for shipment of such cargoes to or from states or non-state actors of proliferation concern, to inspect vessels, aircraft, or other modes of transport reasonably suspected of carrying such cargoes, and to seize such cargoes that are identified.[27]

The PSI does not regularly report on its successes (or failures), but various statements by U.S. government officials have claimed dozens of successes.[28] Information about successes are typically publicized in statements on an *ad hoc* basis. This is due, in part, to the George W. Bush administration's early decision, when crafting the PSI, to maintain some opacity over

[27] "Proliferation Security Initiative: Statement of Interdiction Principles," https://www.psi-online.info/psi-info-en/botschaft/-/2077920

[28] Koch, "Proliferation Security Initiative: Origins and Evolution."

interdictions and avoid embarrassing the parties involved. Public embarrassment had proven less likely to engender cooperation by states involved in an interdiction of proliferation-sensitive goods.[29] One notable, public success was the case of the 2003 interdiction of the *BBC China* ship en route to Libya, which was carrying gas centrifuge parts for Libya's clandestine uranium enrichment program.[30] Complicating the enforcement mission, the ship was German-owned, Antigua and Barbuda-flagged, operating in Mediterranean waters, and had left a port in Dubai. In this case, no complex maritime interdiction needed to be contemplated because the German government "was able to convince the German shipowner to divert the vessel to Italy where the cargo was off-loaded."[31] This PSI interdiction was widely lauded due to the multinational cooperation involved and the fact that it stemmed a major case of nuclear weapons proliferation.

The PSI cannot supersede international law, however, particularly the Law of the Sea. Nevertheless, it is useful as a coordinating, galvanizing, intelligence-sharing, and training effort that gives strength to interdiction efforts for non-proliferation. It can regularly hold a group of states accountable for taking action or failing to do so, and can also be used to hold the participants accountable for failing to incorporate the interdiction principles into national processes and laws.

As a practical matter, and one underlined in various legal analyses of stemming illicit transit of proliferation-sensitive goods, the UN Security Council also bears an activist role in supplementing global frameworks and perpetuating the evolution of international law.[32] Through its passage of Security Council resolutions relevant to preventing illicit transit under certain circumstances, such as the establishment of economic, arms, or sensitive commodity embargos, UNSCRs have supplemented international maritime and airspace law.[33] UNSCRs have included calls to act on the high seas and with regard to suspect aircraft, including under a 2011 arms embargo against Libya under UNSCR 1973. Similar provisions under UN resolutions against Iran and North Korea have pushed international law forward in providing a legal basis to seize illicit shipments, described in more detail below.

The widely varying degree to which countries can control shipments and monitor their border can be seen in the Institute for Science and International Security's *Peddling Peril Index (PPI) for 2019/2020*. The scores achieved by countries under the criterion *Ability to Monitor and Detect Strategic Trafficking,* which includes shipping, ranged from about 10 percent to 76 percent of

[29] Ibid.
[30] Albright, *Peddling Peril* (New York: Free Press, 2010).
[31] Ibid.
[32] Eben Kaplan, "Backgrounder: The Proliferation Security Initiative," *Council on Foreign Relations,* October 19, 2006, https://www.cfr.org/backgrounder/proliferation-security-initiative
[33] Charles Allen, "Countering Proliferation: WMD on the Move," *Georgia Journal of International and Compliance Law,* Vol. 40, No. 15, https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1018&context=gjicl

the available points.[34] The criterion examines a country's general trade environment and customs capabilities, and assigns points for such indicators as the usage of electronic databases to track trade, presence of interagency cooperation, and government outreach. While 29 countries received more than two-thirds of the available points under the criterion, 62 country scores fell below one-third of the points. The United States ranked within the top ten countries.

Countering North Korea's Illicit Shipping Practices

After a prominent incident, the So San case in 2002, in which a North Korean freighter on the way to Yemen was boarded by Spanish forces and found to carry 15 Scud missiles, but had to be released,[35] a number of UNSCRs now allow and even require the inspection and seizure of illicit shipments to and from North Korea. Below, the relevant restrictions are listed, in chronological order by the passing of the resolution. Supporting these UNSCRs are designations lists of shipping companies, vessels, and individuals responsible for sanctions violations.

Paragraph 8 of UNSCR 1718, passed on October 14, 2006, requires UN member states to "prevent the direct or indirect supply, sale or transfer to the DPRK, through their territories or by their nationals, or using their flag vessels or aircraft," of any goods or technology that might assist North Korea's WMD programs. It also prohibits the purchase of such goods from North Korea.

UNSCR 1874, passed on June 12, 2009, toughens the restrictions on imports and exports by calling on states to inspect, seize and dispose of any prohibited goods, and to deny brokering services. The resolution also imposed obligations on flag states to permit inspections, or face being reported to the resolution's Sanctions Committee:

> *12. [The UN Security Council c]alls upon all Member States to inspect vessels, with the consent of the flag State, on the high seas, if they have information that provides reasonable grounds to believe that the cargo of such vessels contains items the supply, sale, transfer, or export of which is prohibited . . . , for the purpose of ensuring strict implementation of those provisions;*

Further, Article 13 specifies that in the case that a flag state does not consent to a boarding on the high seas, it must direct the vessel to a port where the inspection can take place.

Sanctions were progressively tightened under UNSCRs 2087 and 2094. UNSCR 2087, passed on January 22, 2013 urged stricter implementation of search and seizure efforts. UNSCR 2094,

---

[34] David Albright, Sarah Burkhard, and Andrea Stricker, *Peddling Peril Index for 2019/2020: Ranking National Strategic Export Control Systems* (Washington, D.C.: Institute for Science and International Security, 2019), http://isis-online.org/uploads/isis-reports/documents/The_Peddling_Peril_Index_Final_May2019.pdf

[35] Suzanne Goldenberg, John Gittings, and Brian Whitaker, "Sailing on, the Ship with a Hold Full of Scud Missiles," *The Guardian*, December 12, 2002, https://www.theguardian.com/world/2002/dec/12/yemen.northkorea

passed on March 13, 2013, further strengthened the restrictions on North Korean merchant shipping by authorizing states to inspect any cargo being transported to or from North Korea.

Under UNSCR 2270, passed on March 16, 2016, states are not just authorized to inspect cargos, but required to "inspect cargo within or transiting through their territory—including airports, sea ports, and free trade zones" for shipments going to and coming from North Korea.[36] It also requires member states to prohibit the leasing or chartering of their flagged vessels and aircraft to North Korea. Further, member states are required to ban the registering of North Korean vessels and providing them with a flag. For shipments by air, the resolution stipulates that all member states should prohibit "any aircraft to take off from, land at or overfly their respective territories if such aircraft contained items for supply, sale, transfer or export of which were prohibited by all related resolutions, except in cases of emergency landing."[37]

UNSCR 2371, passed on August 5, 2017, extends North Korea's export ban of copper, nickel, zinc, and silver to lead, lead ore, and seafood, and bans all coal exports from North Korea.[38] In her statement on the resolution, former U.S. ambassador to the UN, Nikki Haley, said, "the resolution represented the most stringent sanctions on any country in years."[39]

One month later, on September 11, 2017, the Security Council passed UNSCR 2375, extending the ban on petroleum products trade with North Korea and authorizing the UN Sanctions Committee to designate vessels involved in sanctions violations.

The most recent sanctions resolution to date, UNSCR 2397, passed on December 22, 2017, prohibits the export of vessels from North Korea, caps North Korean petroleum imports, and requires member states to "seize, inspect and freeze any vessel in their ports and territorial waters for involvement in prohibited activities."[40] It prohibits the supply, sale, or transfer of used vessels, and prohibits classification providers, insurance providers, and flag registries to provide their services to "any vessels involved in illicit activities."[41]

However, as the case studies in the following chapter show, North Korea has exploited loopholes and worked actively with witting and unwitting sanctions-evading individuals, companies, and countries to circumvent restrictions. In an Institute analysis of the March 2019 UN Panel of Experts report on North Korea, 56 countries were found to have been involved in sanctions-violating activities during the reporting period. Fourteen of the 56 countries were

[36] United Nations, Press Release, "Security Council Imposes Fresh Sanctions on Democratic People's Republic of Korea, Unanimously Adopting Resolution 2270 (2016)," SC/12267, March 2, 2016, https://www.un.org/press/en/2016/sc12267.doc.htm
[37] Ibid.
[38] United Nations, Press Release, "Security Council Toughens Sanctions Against Democratic People's Republic of Korea, Unanimously Adopting Resolution 2371 (2017)," SC/12945, August 5, 2017, https://www.un.org/press/en/2017/sc12945.doc.htm
[39] Ibid.
[40] United Nations Security Council, "Resolutions," 1718 Sanctions Committee (DPRK), accessed September 9, 2019, https://www.un.org/securitycouncil/sanctions/1718/resolutions
[41] Ibid.

found to have been involved in the evasion of shipping-related sanctions. These violations ranged from failing to de-register sanctioned vessels to facilitating or engaging in ship-to-ship transfers.[42]

Countering Iran's Illicit Shipping Practices

Iran has a long history of illicitly procuring goods for its nuclear, missile, and conventional military programs, and extensive experience in evading and circumventing sanctions via elaborate shipping methods. While the majority of UN sanctions on Iran were lifted with the conclusion of the 2015 nuclear deal, the Joint Comprehensive Plan of Action (JCPOA), and passing of UNSC Resolution 2231 (2015), Iran is still under an international arms and missile embargo, once again subject to major U.S. sanctions, and suppliers are required to use the JCPOA Procurement Channel for many goods relevant to its nuclear program. Because business with Iran involving U.S. goods, services, or nationals is prohibited, Iranian customers looking to purchase U.S.-origin strategic goods must spend significant effort, time, and often money, to ship a good to Iran. Many foreign companies are also wary of conducting business with Iran, in fear of coming under U.S. secondary sanctions. Therefore, Iran tries to use indirect purchases, shipments through intermediary countries and offshore companies, and other clandestine shipping methods to obtain needed goods. Several case studies show the substantial involvement of trading hubs, brokers, shell and trading companies, and overseas bank accounts in such schemes. They further show the associated high payments made to middlemen, the smuggling strategies as they develop, the risks that are taken, and the time and effort that is devoted to hiding the illicit intent from shipping agents and customs agencies in various countries.

[42] See: David Albright, Sarah Burkhard, Bernadette Gostelow, Maximilian Lim, and Andrea Stricker, "56 Countries Involved in Violating UNSC Resolutions on North Korea During Last Reporting Period," *Institute for Science and International Security,* June 6, 2019, http://isis-online.org/isis-reports/detail/56-countries-involved-in-violating-unsc-resolutions-on-north-korea-during-t

Chapter 9. Evasion of Shipping-Related Sanctions and U.S. Enforcement Actions

Stopping an illicit procurement at the point of shipment is much more difficult than at the procurement phase because it leaves fewer observable indicators of illicit activity. If an illicit procurement slips through the export licensing process and receives a license under false pretenses, or the exporter falsely declares that no license is required for a domestically-received shipment and then exports it surreptitiously, scrutiny by customs and shipping companies is often the last chance to catch and seize the items.

The reality is that illicit procurement networks are becoming smarter and are adapting quickly to attempts at detection. The level of scrutiny by border security agents and shipping companies needs to match the ever-evolving layers of concealment efforts by proliferant states and their networks, but also without undue delay to the rapid movement of goods. Their task is to attempt to overcome efforts made to disguise the final destination of a shipment, conceal the contents of packages, or to hide illicit cargo under legitimate goods. Commonly-used methods include falsification of documents and item descriptions, under-valuing of items, removing item identifications such as labels and serial numbers, using flag of convenience registries to avoid oversight during shipment, or using government-owned means of transportation. "Containerization" describes the method of hiding illicitly-obtained items among vast quantities of cargo aboard ships. As explained, ship operators may themselves be involved in the act and disguise ship movements by manipulating the AIS of the ship, including turning it off altogether or displaying a false identity. Ship-to-ship transfers and ship identity fraud methods are increasingly used, especially in sanctions evasion schemes.

A few to many actors could be involved in a single shipment of proliferation-sensitive goods, witting or unwittingly. There are many illicit trade cases investigated by the U.S. government where freight forwarders or port operators were complicit and aided in falsifying documentation. In others, they turned a blind eye to suspicious activity. Many fines accrued by U.S. freight forwarders for strategic trade control violations could have been prevented by using effective screening software that identifies sanctioned entities as illicit recipients of a package. Over time, however, more freight forwarders and other shipping agents appear to have declined services based upon suspicious requests by their customers, and several cases show that illicit procurement networks try to avoid using U.S.-based shipping agents for their illicit trading activities.

A series of case studies follows which demonstrates several of the warning signs and methods employed by illicit procurement networks to ship, divert, and conceal sensitive goods. A focus is on investigation and enforcement opportunities and North Korea's and Iran's sanctions evasion tactics, which often involve elaborate ship-to-ship transfer and commodity concealment schemes.

Case 9.1: Increasingly Elaborate Uses of Ship-to-Ship Transfers by North Korea

According to the March 2019 Panel of Experts report on North Korea, "more than 50 vessels and 160 associated companies" are under investigation for their involvement in illicit ship-to-ship transfers.[1] These numbers illustrate a sharp increase in such transfers during 2018 over previous years. Several cases described by the Panel involved further concealment efforts, including broadcasting a false identity via the vessel's AIS, use of a false ship name, IMO number, or registry, or turning off the AIS altogether.

The Panel's August 2019 mid-term report described in detail two new sanctions evasion tactics, making use of small vessels, or large vessels acting as smaller ones.[2] It found that large vessels conducting ship-to-ship transfers occasionally used a class of AIS transponders designed for small vessels, such as fishing vessels, which are not tracked and monitored as widely as cargo ships. Further, it was observed that actual small vessels, which do not have or do not require an IMO number and other physical identifiers, received cargo during multiple, successive ship-to-ship transfers. Usually at night and over subsequent days, the same small ship would return repeatedly to the larger ship until all the cargo was received, or several different small vessels would share the load.

Using open source AIS information, and information submitted by member states, such as overhead satellite imagery and ground photos, the Panel has actively investigated the misuse of vessels for banned trade. This effort allows the Security Council and Sanctions Committee to hold member states accountable, to designate vessels and networks that are involved, and aids the monitoring of the import caps imposed on North Korea. An incident for which open source AIS data can be found, via *Windward,* a ship-tracking database and maritime intelligence provider*,* shows the steps that the North Korean vessel Kal Ma took to disguise its identity upon entering Chinese coastal waters (see Figure 9.1). Within two days, the vessel changed its broadcasted IMO number, its destination, and its name, before the AIS transmission stopped completely.[3] In a Treasury Department Advisory on North Korea's illicit shipping practices, the Kal Ma is listed as a North Korean-flagged vessel believed to have transported North Korean coal after all coal exports were banned by UNSCR 2371 (2017).[4]

[1] United Nations Security Council, *Report of the United Nations Panel of Experts established pursuant to Resolution 1874 (2009),* S/2019/171, March 5, 2019.
[2] United Nations Security Council, *Report of the United Nations Panel of Experts established pursuant to Resolution 1874 (2009),* S/2019/691, August 30, 2019.
[3] *Report of the Panel of Experts*, March 5, 2019.
[4] See: U.S. Department of Treasury, "Updated Guidance on Addressing North Korea's Illicit Shipping Practices," North Korea Sanctions Advisory, March 21, 2019, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_vessel_advisory_03212019.pdf

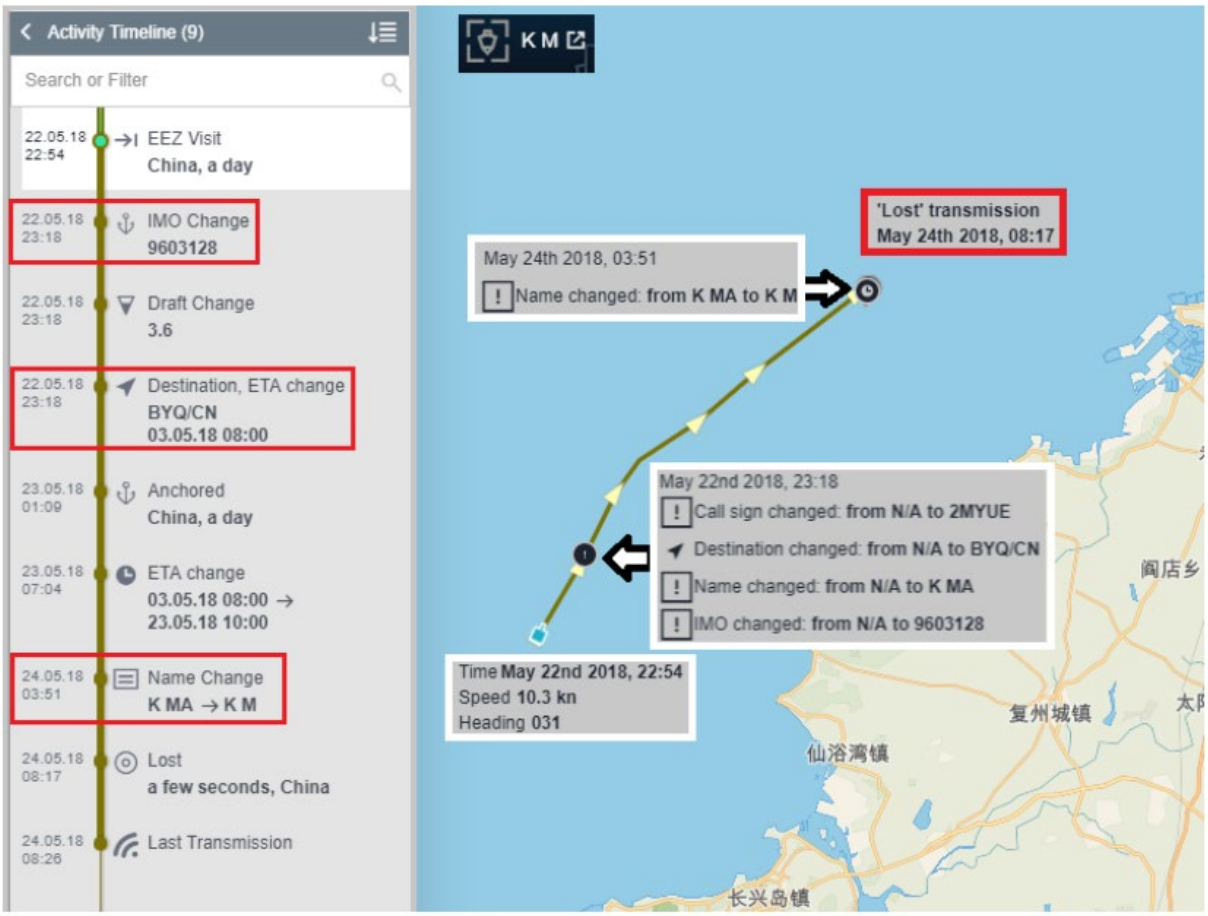


Figure 9.1. Maritime intelligence provider *Windward* captured the steps the vessel Kal Ma took to disguise its identity and route after it had been identified as involved in illicit transports of North Korean coal. Image Source: Windward, via United Nations Security Council, *Report of the United Nations Panel of Experts established pursuant to Resolution 1874 (2009),* S/2019/171.

Another, especially complex, ship-to-ship transfer carried out by North Korea involved the Yuk Tung, a vessel banned globally from ports and registries per UN sanctions. The sanctioned vessel allegedly participated in a ship-to-ship transfer while transmitting another vessel's IMO number, a false name, and a false flag. The "borrowed" IMO number was also painted on the ship's stern. The actual vessel whose IMO number was used had identical physical features to the Yuk Tung, but was 7,000 miles away and also using a false name. Actors working for or with North Korea in countries and territories including the British Virgin Islands, Seychelles, UAE, Singapore, and Taiwan were involved in this scheme and assisted in providing flags and a proclaimed end-user for the oil that likely ended up in North Korea (see Figure 9.2). According to the March 2019 Panel of Experts report, these measures "provided the cover necessary to deceive any of the current, few due diligence and active compliance measures deployed by most global and regional commodity traders [and…] triggered no alerts on the part of the global and regional banks that unwittingly facilitated the multiple financial transactions associated with this transfer or of the insurers and reinsurers that provided protection and indemnity and

hull insurance."[5] The layers of concealment used in this case are showcased in the schematic below.

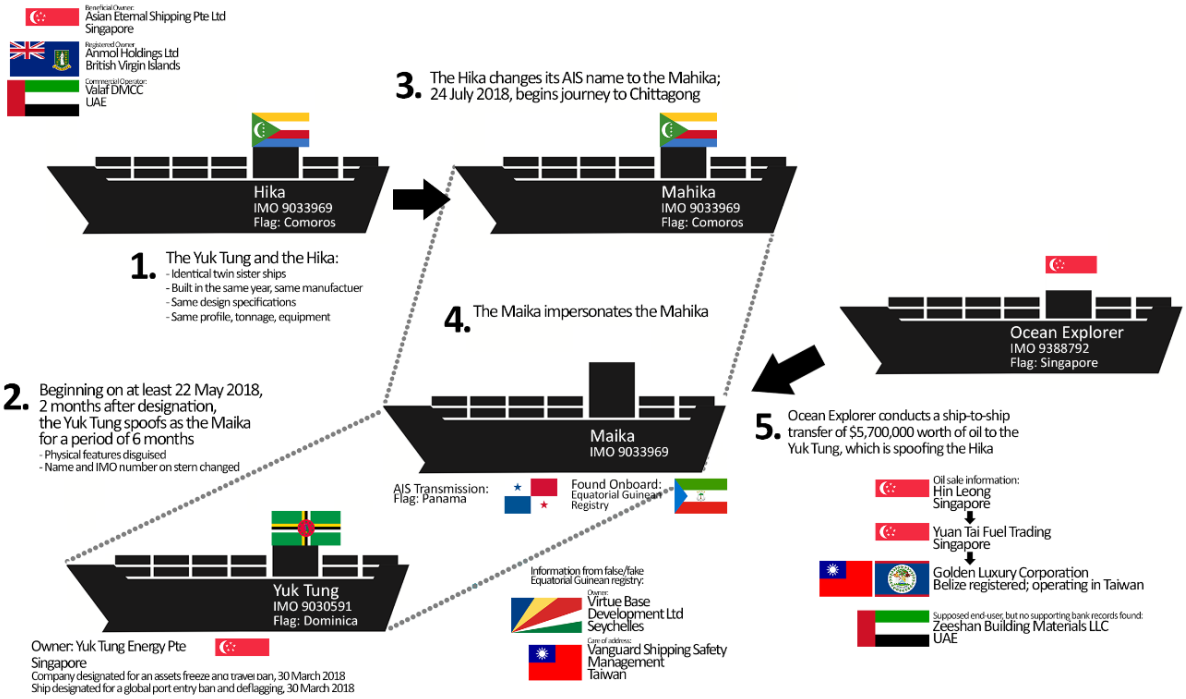


Figure 9.2. Sophisticated ship identity fraud used in the Yuk Tung ship-to-ship transfer.[6]

Case 9.2: Laundering Coal: Selling North Korean Coal as Russian Coal[7]

The media, with the help of research organizations, has done important reporting on sanctions-evasion schemes by North Korea. A March 2018 analysis by *The Washington Post,* with assistance from the Center for Advanced Defense Studies, investigated how North Korean coal was shipped to a nearby port in Russia and then sold as Russian coal to unwitting buyers. The reporting alleged that between August to September 2017, four ships off-loaded North Korean coal at a small port in Kholmsk, Russia, only for the coal to be loaded onto other vessels and "taken to markets" a few days later.[8] Using this scheme, North Korean coal was allegedly sold to unsuspecting customers, including to customers in South Korea and Japan.

[5] *Report of Panel of Experts*, March 5, 2019.

[6] Originally published in: David Albright, Sarah Burkhard, Bernadette Gostelow, Maximilian Lim, and Andrea Stricker, "56 countries involved in violating UNSC Resolutions on North Korea during the last reporting period," *Institute for Science and International Security*, June 6, 2019, http://isis-online.org/uploads/isis-reports/documents/DPRK_Report_June_6%2C_2019_Final.pdf

[7] For more on this case, see: Joby Warrick, "High Seas Shell Game: How a North Korean Shipping Ruse Makes a Mockery of Sanctions," *The Washington Post*, March 3, 2018, https://www.washingtonpost.com/world/national-security/high-seas-shell-game-how-a-north-korean-shipping-ruse-makes-a-mockery-of-sanctions/2018/03/03/3380e1ec-1cb8-11e8-b2d9-08e748f892c0_story.html?noredirect=on

[8] Ibid.

The Scheme

According to *The Washington Post*, one vessel involved was the Yu Yuan, registered in and flying the flag of Togo, and managed and owned by two companies in China. While having different names, the companies, Rich Mountain Trading and Maple Source Shipping, respectively, allegedly shared the same address. On one occasion in early August 2017, the Yu Yuan allegedly departed from northeast China, sailed around South Korea, and as it neared the eastern shore of North Korea, stopped transmitting its AIS-signaled location. It remained "silent" for several days, but was spotted in satellite imagery at the North Korean port of Wonsan. Eleven days after "disappearing," its AIS signal re-appeared at a small port in Nahodka (alternatively, Nakhodka), eastern Russia, where it remained for a few days. The ship reported to the local port authorities that it was coming from Wonsan and carrying coal, but it did not enter the port. Rather, it "remained anchored just beyond the sea wall."[9] This tactic was likely used to obscure the voyage path to maritime observers and perhaps cause the false impression that Nakhodka was the origin of the coal. The Yu Yuan arrived at Kholmsk's coal terminal on September 2, 2017.

On September 21, 2017, another Chinese ship, Sky Angel, arrived in Kholmsk to pick up coal "at the same terminal used by the Yu Yuan."[10] The Sky Angel was flying under the Panamanian flag. The Chinese company managing the ship was located at the same address in the same building as the companies that owned and managed the Yu Yuan. On September 26, 2017, the Sky Angel departed Kholmsk and headed back south-east, to a South Korean port near Soul, where it off-loaded the coal to be delivered to its customers.

The March 2018 Panel of Experts report also detailed the scheme.[11] In addition to the Yu Yuan, the report listed additional three vessels, all North Korea-flagged, that were suspected of having transported coal from North Korea to Kholmsk for laundering between early August and mid-September, and another vessel registered in Sierra Leone suspected of picking up the coal and delivering it to customers. The shipments were allegedly accompanied by false documentation, including a certificate of origin and packing list, published in the annexes of the Panel of Experts report, which claimed the coal was of Russian origin.

Case 9.3: Tankers Disable AIS Signals in the Persian Gulf while Evading Iran Oil Sanctions

A *New York Times* analysis of publicly-available vessel data indicated that several oil tankers turned off their AIS signal when nearing Iran in order to avoid a record of them calling on Iranian ports. The vessels were likely picking up Iranian oil, sanctioned by the United States for

[9] Ibid.
[10] Ibid.
[11] United Nations Security Council, *Report of the United Nations Panel of Experts established pursuant to Resolution 1874 (2009),* March 5, 2018 and its corrigendum, S/2018/171/Corr.1, June 27, 2018.

purchase by most countries. "They don't want to broadcast the fact that they have been in Iran, evading sanctions. It's that simple," the co-founder of a vessel-tracking company was quoted as saying.[12] The report identified five oil tankers that have been observed as "going silent" off the coast of Iran in the Persian Gulf or the Strait of Hormuz: the Sino Energy I, the SC Mercury, the SC Brilliant, the SC Shantou, and the SC Neptune. The ships' movements were then tracked to ports in India and China. All the vessels are Chinese-owned, and the latter four are or were owned by the same company, Sinochem. In many instances, the AIS signal did not return until the ship was on its way out of the Gulf, and the broadcasted draft of the ship was often observed to be lower after the silence, indicating that cargo was loaded in-between. According to a former U.S. Coast Guard officer cited in the report, AIS signals are sometimes lost or turned off for competitive reasons in regions with high activity, but the Persian Gulf is no such region.[13]

Case 9.4: Iranian Ships Go to Great Lengths to Evade U.S. Oil Sanctions

Ship registries are increasingly abandoning business with Iranian-controlled tankers, particularly those involved in UN, EU, and U.S. sanctions violations. According to a U.S. State Department spokesperson quoted by Reuters in July 2019, "Nearly 80 tankers involved in sanctionable activity have been denied the flags they need to sail."[14] The report further stated that Panama de-registered 59 tankers "linked to Iran and Syria" in early 2019 and that countries like Togo and Sierra Leone followed suit and the former de-registered at least three Iranian tankers, and the latter de-registered at least one. The de-flagging often forces Iranian tankers to identify as Iranian and fly under the Iranian flag. This places additional hurdles for them to conduct their illicit business—Iranian-flagged ships draw more attention and may also end up stranded at foreign ports if they run out of fuel. Four Iranian ships were reportedly stranded in Brazil as oil firms refused to sell them fuel in the wake of U.S. sanctions.[15]

According to the Reuters analysis, an Iranian cargo ship named Hayan departed Iran on June 3, 2019, and sailed toward Pakistan's coast. A few days into the journey, the ship changed its name to Mehri II and its flag from Iranian to Samoan. The Samoan government claimed afterward that Samoa's ship registry is closed to foreign-owned vessels and denied ever registering any Iranian ship, indicating that Iran used a false flag. The ship then conducted a ship-to-ship transfer of its cargo before changing its flag and name back to the original ones and returning home.[16] While the method of using false flags may occasionally work for Iran, it also

[12] Michael Forsythe and Ronen Bergman, "To Evade Sanctions on Iran, Ships Vanish in Plain Sight," *The New York Times,* July 2, 2019, https://www.nytimes.com/2019/07/02/world/middleeast/china-oil-iran-sanctions.html
[13] "To Evade Sanctions on Iran, Ships Vanish in Plain Sight."
[14] Jonathan Saul, Parisa Hafezi, Marianna Parraga, "Flags of Inconvenience: Noose Tightens around Iranian Shipping," Reuters. July 26, 2019, https://www.reuters.com/article/us-mideast-iran-tanker-flags-insight/flags-of-inconvenience-noose-tightens-around-iranian-shipping-idUSKCN1UL0M8?utm_source=In+Escalation%2C+Iran+Tests+Medium-Range+Missile%2C+U.S.+Official+Says&utm_campaign=eye-on-iran&utm_medium=email
[15] Ibid.
[16] Ibid.

subjects its tankers to interdictions, foreign boarding, and seizures, as any ship on the high seas would which lacks a proper or confirmed country flag. The Iranian tanker with a false flag would become subject to the jurisdiction of that state, or by any government authority that it may come across.

Case 9.5: U.S. Seizure of a North Korean Sanctions-Evading Vessel

A seizure by the United States of a North Korea sanctions-busting ship, the M/V Wise Honest, shows an innovative method of extraterritorially enforcing procurement, shipping, and financial sanctions. Further, it shows that North Korea is willing to go to great lengths in order to export coal, which is a key source of revenue for sanctioned North Korean nuclear, missile, and military programs.[17]

UN Security Council Resolutions 2321 (2016)[18] and 2371 (2017) prohibit the import and export of North Korean coal and other materials. Since 2017, North Korean total exports have decreased by 86.3 percent.[19] North Korea relies on the assistance of foreign governments and illicit agents abroad to facilitate its banned trade and to obtain heavy machinery that it cannot produce domestically. Entities in China and Russia have played a vital role in facilitating the illegal transshipment and import of illicit goods from North Korea. In the M/V Wise Honest case, in one instance, Russian entities helped to falsify shipping documentation. This case highlights the need for Russia, China, Indonesia, and other states where illicit transshipment and imports occur to abide by international sanctions and to enforce their national legislation to prevent illicit trade.

On May 9, 2019, the U.S. Department of Justice announced the filing of a civil forfeiture complaint against the North Korean bulk cargo carrier, "M/V (Maritime Vessel) Wise Honest," pursuant to violations of the International Emergency Economic Powers Act (IEEPA).[20] Between November 2016 and April 2018, M/V Wise Honest was allegedly used by the Pyongyang Korea Songi Shipping Company, its registered owner, to illegally export North Korean coal elsewhere, violating UN Security Council resolutions and IEEPA. Via transshipment, and in exchange, the vessel imported heavy machinery back to North Korea for delivery to the Korea Songi General Trading Corporation. A U.S. Complaint alleges that the M/V Wise Honest and the conspirators

---

[17] *Verified Complaint: United States of America v Bulk Cargo Carrier known as the "Wise Honest," Bearing International Maritime Organization Number 8905490*, May 7, 2019, https://int.nyt.com/data/documenthelper/851-wise-honest-complaint/17839ee8c606711f6ded/optimized/full.pdf#page=1

[18] UN Security Council, *Security Council Strengthens Sanctions on Democratic Republic of Korea, Unanimously Adopting Resolution 2321 (2016)*, SC/12603, November 30, 2016, https://www.un.org/press/en/2016/sc12603.doc.htm

[19] Lee Kwan Kyo, "Gross Domestic Product Estimates * for North Korea in 2018," Bank of Korea, July 26, 2019, https://www.bok.or.kr/eng/bbs/E0000634/view.do?nttId=10053001&menuNo=400069

[20] U.S. Department of Justice, "North Korean Cargo Vessel Connected to Sanctions Violations Seized by U.S. Government," May 9, 2019, https://www.justice.gov/opa/pr/north-korean-cargo-vessel-connected-sanctions-violations-seized-us-government ; *Verified Complaint: United States of America v Bulk Cargo Carrier known as the "Wise Honest."*

illegally used U.S. financial institutions to transmit U.S dollar payments for M/V Wise Honest operations and that M/V Wise Honest was used to smuggle coal to or via China, Russia, Indonesia, and possibly South Korea.

M/V Wise Honest is the only registered vessel of the Korea Songi Shipping Company, which is an affiliate of Korea Songi General Trading Company (aka Songi Trading Company). Songi Trading Company was identified by OFAC as subordinate to the Korean People's Army. On June 1, 2017, OFAC designated Korea Songi General Trading Company.[21]

On April 1, 2018, the Indonesian Ministry of Transportation detained M/V Wise Honest on suspicion of UN sanctions violations. On July 17, 2018, the United States issued a warrant for its seizure.[22] On November 22, 2018, the captain of M/V Wise Honest, a North Korean national, was convicted by the state court of Balikpapan, Indonesia, for providing false vessel documentation. The M/V Wise Honest was in the custody of the United States, reportedly in American Samoa, until it was approved for an interlocutory sale and sold at auction.[23] The forfeiture of the vessel by the U.S. government became official on October 21, 2019.[24]

The complaint cites Kwon Chol Nam, a North Korean national, as a representative and a "point of contact" for Korea Songi Shipping Company, where he allegedly served as the coordinator for the shipment and payment (in U.S. dollars) for the Korea Songi scheme and managed the operations of M/V Wise Honest. The conspirators allegedly gained access to the U.S. financial system and routed payments through banks located in the Southern District of New York. The complaint indicates that Kwon was aware of the restrictions on North Korean coal exports/machinery imports, as well as restrictions on North Korea's use of the U.S. financial system.

Additionally, the UN Panel of Experts on North Korea identified Hamid Ali, an Indonesian commodity trader and broker, and Jong Song Ho, the President of Jinmyong Trading Group and Jinmyong Joint Bank of the Democratic People's Republic of Korea (DPRK), as well as a third broker, Eko Setyatmoko, as three main figures in facilitating the March 2018 coal export.[25] Eko Setyatmoko operated a shipping company called Pt. Bara Makmur Sadayana. Ali was allegedly

---

[21] *Verified Complaint: United States of America v Bulk Cargo Carrier known as the "Wise Honest,"* p. 9.
[22] Ibid, p. 24.
[23] "U.S. Seizes North Korean Cargo Ship for Violating Sanctions," CBS News/The Associated Press, https://www.cbsnews.com/news/north-korean-cargo-ship-seized-by-us-wise-honest-for-violating-sanctions-today-2019-05-09/ ; U.S. Marshals Service, " Sale of 'WISE HONEST'," https://www.usmarshals.gov/assets/2019/wise-honest.pdf; "Wise Honest, North Korean Cargo Ship Seized by U.S., Sold in Sealed Auction," The Associated Press. October 9, 2019, https://www.washingtontimes.com/news/2019/oct/9/wise-honest-north-korean-cargo-ship-seized-us-sold/
[24] U.S. Department of Justice, Press Release, "Department of Justice Announces Forfeiture of North Korean Cargo Vessel," October 21, 2019, https://www.justice.gov/opa/pr/department-justice-announces-forfeiture-north-korean-cargo-vessel
[25] *Report of Panel of Experts*, March 5, 2019.

introduced to Jong Song Ho while attending regular meetings with diplomats at the North Korean Embassy in Jakarta, Indonesia.[26]

The Korea Songi scheme used a number of methods to deceive authorities. Since August 4, 2017, M/V Wise Honest had not activated its AIS, effectively concealing the ship's movements, in violation of international law. The conspirators also attempted to deceive authorities by "double-flagging" (false-flagging) M/V Wise Honest in order to disguise the true identity and North Korean origin of the vessel. M/V Wise Honest was incorrectly registered under multiple jurisdictions, including Tanzania[27], Sierra Leone[28], and possibly others. In at least one instance, ship-to-ship (STS) transfers, or transfers of commodities between ships at sea, were intended to be used to transport the coal into ports of entry.[29]

Coal Exports

On November 15, 2016, Kwon arranged for M/V Wise Honest to depart the Nam Pho Port (alternatively, Nampo) with 26,393 tons of anthracite coal for delivery to an unnamed Chinese port. On December 19, 2016, Kwon again arranged for M/V Wise Honest to depart Nampo with 26,550 tons of anthracite coal for delivery to an unnamed Chinese port. In another instance, Kwon arranged for M/V Wise Honest to depart Nampo with coal, where it would be diverted through a Russian port onto its final destination. While at the Russian port, rather than in North Korea, cargo documentation was prepared for M/V Wise Honest. Meanwhile, numerous U.S. dollar payments were illicitly transmitted through the U.S. financial system to pay for equipment, supplies, and the upkeep of the vessel.

No information is available regarding the M/V Wise Honest activities and whereabouts between January and December 2017. In December 2017, Hamid Ali was introduced to Jong Song Ho, the President of Jinmyong Trading Group and Jinmyong Joint Bank in North Korea. A month later, Ali and Ho began to scheme to transship coal for a March 2018 export (Figure 9.3). After the total ban on North Korean coal exports was adopted by the Security Council, the illicit coal export required more careful planning. Twenty-eight to thirty separate payments totaling $760,000 from the bank account of a company named Huitong Minerals were wired through U.S. financial institutions located in New York to Ali's account to pay for the service. Eko Setyatmoko received at least an unspecified portion of this payment.

On March 14, 2018, M/V Wise Honest left Nampo, North Korea, towards Indonesia with 25,500 tons of anthracite coal. Documentation cited Hong Kong Nova International Trade Company, a cigarette-machinery manufacturer, as the seller of the coal. According to documentation obtained by Indonesian authorities, a Russian cargo ship planned an STS transfer with M/V Wise Honest off the coast of Teluk Balikpapan in East Kalimantan, Indonesia, where the shipment

[26] Ibid, p. 24.
[27] *Verified Complaint: United States of America v Bulk Cargo Carrier known as the "Wise Honest,"* p. 16.
[28] *Report of the Panel of Experts*, March 5, 2019, p. 23.
[29] Ibid, p. 24.

would be shipped to Pohang, Republic of Korea (ROK), and delivered to Enermax, a company located in the ROK. However, further information obtained by the UN Panel of Experts revealed that the M/V Wise Honest planned an STS transfer with the Ken Orchid (IMO No. 9598153), operated by Qingdao Global Shipping Co. Ltd., aka Qingdao Global Shipping Group Ltd, based out of Shandong, China, which received a payment from a bank account associated with the M/V Wise Honest' operations.[30] Enermax denied any role in the scheme.[31] The total value of this coal shipment was estimated at $2,990,000.[32] Falsified documentation indicated that the coal shipment was exported from Nahkoda, Russia (the same port reported to allow vessels involved in the Kholmsk scheme to linger) instead of from Nampo, North Korea.

In November 2018, the District Court in Balikpapan, Indonesia, issued a court order requesting the March 2018 illicit coal shipment be returned to the original Indonesian broker, Eko Setyamoko. A midterm report issued by the UN Panel of Experts, released on August 30, 2019, alleged that the 25,500 metric tons of illicit anthracite coal were transferred from the M/V Wise Honest to a bulk cargo carrier known as the M/V Dong Thanh, registered in Panama (IMO No. 9180035) and operated by Qingdao Global Shipping Co. Ltd (aka Qingdao Global Shipping Group Ltd.). The coal was shipped by Pt. Bara Makmur Sadayana for delivery to Malaysia. On April 13, 2019, Qingdao Global Shipping Co. Ltd. directed the M/V Dong Thanh to enter the Malaysian port of Kemaman.

On April 19, 2019, the Dong Thanh was refused entry into the Port of Kemaman by Malaysian authorities. Malaysian authorities alleged that the anthracite coal shipment documentation and certificates of origin prepared by the shipper, Pt. Bara Makmur Sadayana (a company operated by Setyatmoko), were manipulated to falsely claim that the coal's origin was Indonesia. Following this, the M/V Dong Thanh sailed for Ba Ria-Vung Tau, Vietnam and arrived on June 6, 2019, where Vietnamese customs officials interdicted the vessel.

[30] *Report of the Panel of Experts*, August 30, 2019.

[31] Shim Kyu-Seok, "Local Company Probed for Buying Coal," *Korea JoongAng Daily*, July 17, 2019. http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3065574

[32] *Report of the Panel of Experts*, p. 24.

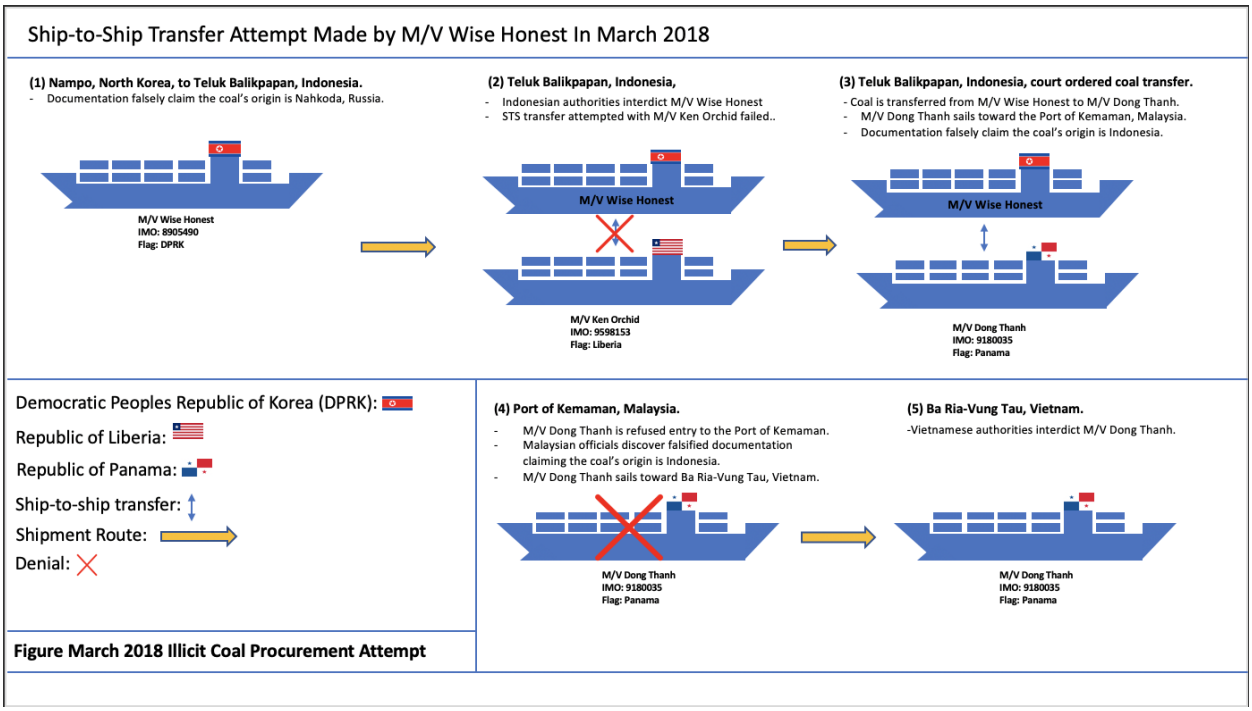


Figure 9.3. March 2018 procurement path of the shipment from Nampo, North Korea, to Indonesia and the attempted ship-to-ship transfer in the Balikpapan Bay.

On December 10, 2018, South Korea indicted four nationals and five commodity trading companies in connection with the Korea Songi scheme. The Public Prosecutors Office noted that the motive for their involvement in the Korea Songi scheme was "profit from arbitrage, using the fact that the prices of North Korean coal and other materials are low due to their difficulty to be traded internationally."[33]

Machinery Imports

On November 1, 2016, Kwon arranged for M/V Wise Honest to ship heavy machinery, including an overflow ball mill, a pendulum feeder, a "down the hole drill," a "cone crusher," and 412,584 kilograms of steel plates from Yantai Port in Shandong, China to "Korea Songi General Trading Corporation" at "NAMPO PORT, D.P.R K." In this instance, the nationality of the vessel was registered as "Tanzania." On January 25, 2017, Kwon and two additional co-conspirators arranged for M/V Wise Honest to transport eight "off road dump truck," three "pkgs of spare parts," 30 tires, and "I truck crane QY75K in 4 parts," for delivery to Korea Songi Trading Corporation at Nampo Port, North Korea.

[33] Joyce Lee, "South Korean prosecutors indict four for importing North Korean coal," Reuters. December 10, 2018, https://www.reuters.com/article/us-northkorea-southkoreacoal/south-korean-prosecutors-indict-four-for-importing-north-korean-coal-idUSKBN1O90TP

Case 9.6: DHL Held Accountable for Assisting Unauthorized Shipments to Syria, Sudan, and Iran

In 2009, following a five and a half year investigation, DPWN Holdings (USA) Inc. (formerly DHL Holdings (USA), Inc.) and DHL Express (USA), Inc., collectively DHL, reached a $9.4 million settlement with OFAC and the Department of Commerce's Bureau of Industry and Security (BIS) over alleged violations of U.S. sanctions laws and export control regulations. Between 2002 and 2007, the company allegedly violated the Iranian Transactions and Sanctions Regulations (ITSR or ITR), Sudanese Sanctions Regulations (SSR), Reporting, Procedures and Penalties Regulations (RPPR), and Export Administration Regulations (EAR) on numerous counts.[34]

According to the settlement agreement, DHL violated the EAR on 98 occasions by failing to comply with recordkeeping requirements and "causing, aiding, or abetting" exports to Syria without a license.[35] Specifically, DHL allegedly "failed to retain air waybills and other export control documents" for 90 export transactions from the United States to Syria, occurring on or about two dates in 2004.[36] On eight occasions on or about two separate dates in 2004, DHL transported EAR-controlled items subject to Commerce Department licensing requirements to Syria without the required license. The Proposed Charging Letter from BIS to DHL listed the involved items as: Water Purification Equipment (two exports), Vehicle monitoring system (two exports), Re-agent particles, Cable charger, Designer eye glass frames (no lenses), and Power supply parts.[37]

The alleged OFAC violations included over 300 unlicensed shipments to Iran and Sudan between August 2002 and March 2007 and failure to maintain records for numerous other shipments to Iran, occurring between December 2002 and April 2006.[38] Initially, according to a 2008 OFAC Prepenalty Notice, DHL was accused of: exporting or attempting to export four "shipments of merchandise" to Sudan and 63 shipments to Iran without the required licenses, importing one shipment of merchandise from Iran without a license, and failing to maintain cargo descriptions for 32,228 exports to Iran between August 15, 2002, and April 17, 2006.[39] The U.S. Department of Homeland Security's Customs and Border Protection (CBP) intercepted many of the shipments, reported to OFAC, and assisted in the investigation.[40]

---

[34] U.S. Department of Treasury, Press Release, "U.S. Treasury and Commerce Departments Announce $9.4 Million Settlement with DHL," August 6, 2009, https://www.treasury.gov/press-center/press-releases/Pages/tg259.aspx

[35] U.S. Department of Commerce, *Order Relating to DPWN Holdings (USA), Inc. and DHL Express (USA), Inc.,* August 6, 2009.

[36] Ibid.

[37] U.S. Department of Commerce, DHL Schedule of Violations, Schedule B of "Proposed Charging Letter," Exhibit B, *Order Relating to DPWN Holdings (USA), Inc. and DHL Express (USA), Inc.*

[38] "U.S. Treasury and Commerce Departments Announce $9.4 Million Settlement with DHL."

[39] U.S. Department of Treasury, "Prepenalty Notice," October 2, 2008, Exhibit A, *Order Relating to DPWN Holdings (USA), Inc. and DHL Express (USA), Inc.*

[40] "U.S. Treasury and Commerce Departments Announce $9.4 Million Settlement with DHL."

The Prepenalty Notice lists four aggravating factors and three mitigating factors for the unlicensed exports and import, and an additional mitigating factor for the failures to keep required records. The aggravating factors included that DHL had "reason to know" about the imminent violations upon entering the shipment data for Iran and Sudan into its database; the shipments may have brought "a significant economic benefit to sanctioned countries" and may have harmed the "sanctions program objectives"; DHL "did not have an effective OFAC compliance program"; and the violations showed a "large pattern of misconduct over an extended period of time."[41] The mitigating factors included cooperation with OFAC by "providing relevant information […] to the extent such information existed"; an improved compliance program after 2006; and agreeing to wave the statute of limitations.[42] A unique mitigating factor for the record-keeping violations was that "as much of 90 percent" of the unrecorded shipments were likely "shipments of informational material, which were not prohibited by the ITR."[43]

OFAC further noted that it was not able to propose a penalty proportional to the transaction values of the unauthorized shipments, because of missing records for most of the shipments, which is why OFAC proposed the maximum civil penalty at the time of the violations.[44] Conclusively, according to the settlement agreement, a 2009 response by DHL "appears to show that DHL committed a total of 309 violations of the ITR, four violations of the SSR, and more than 9,000 violations of the RPPR."

A list of items shipped to Iran and Sudan in violation of the ITR and SSR was included in the 2008 Prepenalty Notice and showed a range of item descriptions, including computer software, medical equipment, and cosmetics. According to the Treasury Department, complete records of shipments need to be maintained for five years and the shipment of most goods to Iran and Sudan is prohibited by OFAC regulations. Further, thousands of related airway bills were allegedly missing descriptions of the packages' contents.[45]

In addition to the settlement payment, DHL agreed to undergo an external audit of its compliance with U.S. export controls and sanctions laws.[46]

Case 9.7: FedEx Held Accountable for Several Deliveries to Two Sanctioned Entities

In 2017, the Federal Express Corporation (FedEx), operating as FedEx Express in Memphis, Tennessee, was charged with 53 violations of the Code of Federal Regulations as spelled out under 15 CFR 764.2(b), the section that criminalizes the "causing, aiding, or abetting" of any

[41] "Prepenalty Notice," October 2, 2008.
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] "U.S. Treasury and Commerce Departments Announce $9.4 Million Settlement with DHL."
[46] *Order Relating to DPWN Holdings (USA), Inc. and DHL Express (USA), Inc.*

EAA or EAR violation.[47,48] According to the charges laid out in the U.S. Commerce Department order, FedEx "facilitated the export of civil aircraft parts and equipment used for electron microscope manufacturing […] without the required BIS licenses" to two entities designated on the BIS Entity List.[49] The items were classified with the export control classification number (ECCN) 9A991 or 7A994 or controlled under the EAR99 regulation, and were sent from the United States to the sanctioned entities in France and Pakistan between on or about July 1, 2011, and on or about January 19, 2012.

FedEx was held liable as party of the transaction and for "providing carrier services or both carrier and freight forwarding services" for the illegal exports.[50] It was further accused of using "proprietary screening software that failed to flag or detect close matches to the Entity List listings" for the two entities.[51]

The first illicit entity, Aerotechnic, is based in France and has been listed on the BIS Entity List since June 28, 2011. The Federal Register, which announced the addition of *Aerotechnic France SAS* to the list, shows that two affiliated entities with the same address were also listed.[52] The three entities were listed after they were charged on June 23, 2011 for allegedly conspiring to "illegally export military components for fighter jets and attack helicopters" to Iran. [53] The Schedule of Violations as part of the Charging Letter from BIS to FedEx listed the commodities with their values that were illegally transported by FedEx. The commodity descriptions ranged from "Aircraft parts – Relay," valued at $8,963, and "Aircraft parts - Pressure Switch," valued at $5,000, to "Protruding Head Bolt," valued at $50.[54]

PINSTECH, the Pakistan Institute of Science and Technology, is known for its affiliation with the Pakistan Atomic Energy Commission and for hosting the laboratories in which the Pakistani government separates plutonium for its nuclear weapons.[55] According to the BIS Order, PINSTECH was added to the Entity List on November 19, 1998, "shortly after Pakistan

[47] U.S. Department of Commerce, *Order Relating to Federal Express Corporation d/b/a FedEx Express*, issued April 24, 2018.
[48] Electronic Code of Federal Regulations (e-CFR), *Title 15 § 764.2*. Available at: https://www.law.cornell.edu/cfr/text/15/764.2
[49] *Order Relating to Federal Express Corporation d/b/a FedEx Express*.
[50] Ibid.
[51] Ibid.
[52] U.S. Department of Commerce, "Addition of Certain Persons on the Entity List," *Federal Register* 76, no. 124, June 28, 2011, https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/312-76-fr-37632/file
[53] U.S. Department of Justice, Press Release, "Members of International Procurement Network Indicted for Supplying Iran with U.S. Military Aircraft Components," June 23, 2011, https://www.justice.gov/opa/pr/members-international-procurement-network-indicted-supplying-iran-us-military-aircraft
[54] See: U.S. Department of Commerce to Federal Express Corporation, *Charging Letter,* December 14, 2017.
[55] David Albright and Paul Brannan, "Pakistan Expanding Plutonium Separation Facility Near Rawalpindi," *Institute for Science and International Security*, May 19, 2009, https://isis-online.org/uploads/isis-reports/documents/PakistanExpandingNewLabs_19May2009.pdf

detonated a nuclear device."[56] According to the Schedule of Violations, the illegal transport of "equipment for electron microscope manufacturing" was valued at $10,127.96.[57] According to the BIS Order, FedEx should have been able to identify the designation of Aerotechnic and PINSTECH based on information the exporter provided to FedEx regarding the shipment. The exporter allegedly "provided name and address or location information regarding these transactions," which identified Aerotechnic as "Aerotechnic," "Aerotechnic France," or "Aerotechnic-France," and PINSTECH as "PINSTECH."[58] Further, the address used for Aerotechnic "matched or nearly matched" the information provided on the Entity List including city name, zip code, street name, and building number.[59] For PINSTECH, the city name allegedly matched as well.

BIS alleged that FedEx "knew or should have known" that its screening software would not return a warning for a company whose name is an almost identical match with the information provided by the Entity List, even if the address was a direct match or almost identical.[60] BIS concluded that the software did not flag the company because Aerotechnic was listed on the Entity List as Aerotechnic France *SAS*. According to the BIS Order, SAS is a "non-differentiating term" such as the English "LLC."[61] Further, the software did not flag a direct match of the acronym PINSTECH with information provided by the Entity List.

FedEx and BIS entered into a settlement agreement on April 23, 2018. According to the agreement, FedEx was fined a civil penalty of $500,000. It further agreed to have its export control compliance program audited for the fiscal years 2017 through 2020.[62]

As discussed earlier, a complaint by FedEx against the Department of Commerce, Secretary of Commerce Wilbur Ross, Assistant Secretary of Industry and Analysis, Nazak Nikakhtar, and BIS, regarding the carrier's legal responsibility to comply with all aspects of the EAR, has so far not been successful. The complaint states, "The determination of whether the tendered package contains an 'item subject to the EAR' and whether a license is required are virtually impossible for common carriers to comply with."[63] It further cites the Due Process Clause of the U.S. Constitution's Fifth Amendment and privacy-infringement consequences it may face "from customers and foreign governments," would it "police the contents and ultimate destinations of the missions of daily shipments to ensure compliance with the EAR."[64] The Commerce Department filed a motion to dismiss the case.[65]

---

[56] *Order Relating to Federal Express Corporation d/b/a FedEx Express*.
[57] U.S. Department of Commerce to Federal Express Corporation, *Charging Letter,* December 14, 2017.
[58] *Order Relating to Federal Express Corporation d/b/a FedEx Express*.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] U.S Department of Commerce and Federal Express Corporation, *Settlement Agreement*, April 23, 2018.
[63] FedEx Corporation, *Complaint for Declaratory, Injunctive, and other Relief*, June 24, 2019, https://f.datasrvr.com/fr1/519/97413/FedEx_v_Dept._of_Commerce_Complaint.pdf
[64] *Complaint for Declaratory, Injunctive, and other Relief*.
[65] Max Garland, "U.S. Department of Commerce Calls for FedEx Lawsuit over Export Rules to be Dismissed," *Memphis Commercial Appeal*, September 11, 2019,

Case 9.8: Kinetsu World Express Held Accountable for Assisting an Export to a Sanctioned Entity in China

On September 23, 2014, BIS and Kinetsu World Express (USA),Inc. (KWE) entered into a settlement agreement regarding KWE's alleged violation of Title 15 of the Code of Federal Regulations SS 764.2(b), which criminalizes the "causing, aiding, or abetting an act prohibited by the [Export Administration] Regulations."[66] According to the Proposed Charging Letter, KWE acted as a freight forwarder in an unauthorized export from the United States to China of items regulated under EAR99. The declared recipient of the items, described as "three spiral duct production machines and related accessories," was China National Precision Machinery Import/Export Corporation (CPMIEC), an entity on the Treasury Department's SDN List.[67] CPMIEC was added to the SDN List on June 13, 2006 for its involvement in supplying sanctioned Iranian entities with missile-related and dual-use items.[68] Its entry on the SDN List carried the special identifier "NPWMD," which is used for "Weapons of Mass Destruction Proliferator and Their Supporters." As such, a license for the export of any items would have been required.[69] Further, CPMIEC was subject to an import ban and State Department sanctions.[70]

According to the Proposed Charging Letter, KWE did not screen any designated parties lists when it "arranged for the shipment" and filed the export of the items valued at least $250,000 in the Automated Export System (AES). Instead, it incorrectly stated that the export fell under "NRL," meaning "No License Required." As part of the settlement, KWE agreed to pay a civil penalty of $30,000.[71]

Case 9.9: General Logistics International Held Accountable for Delivering to a Sanctioned Entity in Pakistan

On January 26, 2015, BIS and General Logistics International, Inc. (GLI) entered into a settlement agreement regarding GLI's alleged violations of Title 15 of the Code of Federal Regulations SS 764.2(b), which criminalizes the "causing, aiding, or abetting an act prohibited by the [Export Administration] Regulations."[72] Specifically, GLI was accused of having "facilitated the export of scrap steel […] with a total value of approximately $672,022" to a designated entity in Pakistan.[73] According to the Schedule of Violations as part of the Proposed

https://www.commercialappeal.com/story/money/industries/logistics/2019/09/11/fedex-sues-commerce-department-export-administration-regulations/2290695001/

[66] U.S. Department of Commerce and Kintetsu World Express, *Settlement Agreement,* September 23, 2014.
[67] U.S. Department of Commerce to Kinetsu World Express, *Proposed Charging Letter*, undated.
[68] U.S. Department of the Treasury, Press Release, "Treasury Designates U.S. and Chinese Companies Supporting Iranian Missile Proliferation," June 13, 2006, https://www.treasury.gov/press-center/press-releases/Pages/js4317.aspx
[69] U.S. Department of Commerce to Kinetsu World Express, *Proposed Charging Letter*.
[70] "Treasury Designates U.S. and Chinese Companies Supporting Iranian Missile Proliferation," June 13, 2006.
[71] U.S. Department of Commerce and Kintetsu World Express, *Settlement Agreement.*
[72] U.S. Department of Commerce and General Logistics International, *Settlement Agreement,* January 26, 2015.
[73] Ibid.

Charging Letter, four exports of varying quantities of scrap steel took place on four different dates in November 2009.[74] The recipient, People's Steel Mills, is listed on the Entity List administered by BIS and the exports therefore fall under EAR99 and would have required a license. GLI allegedly acted on behalf of a Canadian company when it "arranged for the trucking […] from the U.S. exporter's location to the port of export, arranged for the shipping […] and prepared and submitted shipping documentation."[75] The declaration filed in the Automated Export System showed that the export was incorrectly designated by GLI as "NRL," meaning "No License Required." As part of the settlement, GLI agreed to pay a civil penalty of $90,000.

[74] U.S. Department of Commerce to General Logistics International, *Proposed Charging Letter*, undated.
[75] Ibid.

Chapter 10. Transshipping Strategic Goods through Intermediaries

Shipping goods indirectly through multiple destinations is a tactic frequently used to illicitly ship strategic goods from a vigilant supplier country to a proliferant state. Transshipment, in its simplest form, is the shipping of a good from location A to location B, and then to location C. The transshipment point B, or initial recipient of the goods, can be a distributor or trading company in an intermediary country, a special economic zone, or a middleman located within the supplier state. Often, goods are stored for a limited time period at the transshipment point, new shipping arrangements are made, and goods are re-packaged. Meanwhile, the supplier is led to believe that the transshipment point is the final end destination.

Case 10.1: GPS-Tracking Reveals Shipments Made to Turkey Ended Up in Iran

On January 1, 2019, Aiden Davidson, aka Hamed Aliabadi, a dual U.S.-Iranian citizen, was indicted by a Grand Jury in the U.S. District Court for the District of New Hampshire, on charges relating to the unauthorized export of goods from the United States to Iran.[1] Davidson was charged with ten counts of money laundering, nine counts of smuggling goods from the United States, and one count each of conspiracy to violate IEEPA, carry out international money laundering, and unlawfully procure naturalization. Davidson was accused of using his company, Golden Gate, LLC, to purchase and export goods intended for Iran, via transshipment through a third country, and receive payments from Iran for the goods and services provided. Investigators found that Golden Gate was registered at Davidson's home in New Hampshire. In the same indictment, the Iranian customer, Babazadeh Trading, aka Babazadeh Hydraulic Trading Group, a trading company in Tehran, was also indicted on one count of IEEPA conspiracy and one count of international money laundering conspiracy. Davidson pleaded not guilty.[2] The trial date, originally scheduled for September 2019, was postponed for February 4, 2020.

This case first came to light on August 31, 2018, when a U.S. special agent of the Department of Homeland Security (DHS), Homeland Security Investigations, filed a criminal complaint in the same district court, accusing Davidson of "conspiracy to willfully violate the Iranian Transactions and Sanctions Regulations (ITSR)."[3] Davidson was arrested shortly after and released on bail and was forced to wear GPS monitoring while awaiting trial.[4]

---

[1] United States District Court in the District of New Hampshire, *Indictment: United States of America v. Aiden Davidson and Babazadeh Trading Co.*, 18 CR 169 (2019), Filed January 9, 2019. Available at Pacer.gov

[2] Adam Rawnsley and Seamus Hughes, "Feds Broke Up Alleged Scheme to Send Surplus Pentagon Gear to Iran," *The Daily Beast,* May 21, 2019, https://www.thedailybeast.com/new-hampshire-man-allegedly-tried-to-send-iran-a-million-dollars-of-pentagon-goods

[3] United States District Court in the District of New Hampshire, *Affidavit in Support of Application for Arrest Warrant, United States of America v. Aiden Davidson,* Criminal Complaint, Filed August 31, 2018. Available at https://www.pacer.gov/

[4] "Feds Broke Up Alleged Scheme to Send Surplus Pentagon Gear to Iran."

The complaint accused Davidson of conspiring to "export and cause to be exported, directly or indirectly […] heavy machinery equipment" from the U.S. to Iran without the required export license and of engaging in "transactions that evade or avoid, or have the purpose of evading or avoiding, any of the prohibitions contained in the ITSR, including prohibitions against the unauthorized exportation of goods from the United States to a third country if the goods are intended or destined for Iran."[5] Per the ITSR, the items Davidson allegedly exported to Iran via Turkey, which, according to the complaint, included Department of Defense (DOD) surplus equipment, would have required authorization from the Treasury Department's Office of Foreign Assets Control (OFAC), as do all exports from the United States intended for Iran. The OFAC licensing record allegedly revealed no indications that Davidson or his company ever applied for an export license to Iran for the shipments.

This case shows how vigilance by export authorities offers unique opportunities for detection and to follow the path of illicit procurements, as well as to seize banned goods at the shipping stage. Authorities in this case used export data to investigate purported end-users and determine that they were possibly diverting goods onward to Iran.

Findings from the Investigation

Davidson and his alleged Iran export scheme have been under investigation by the Department of Commerce (DOC) and DHS since 2016. The investigation appears to have been set off by Commerce Department suspicions about a proclaimed end-user in Turkey in two Electronic Export Information (EEI) filings that Davidson made in the Automated Export System (AES). An EEI filing needs to identify the final destination and end-user, however, from the alleged recipient's website, investigators found that the recipient actually operates as a freight forwarder and logistics company. They further found that the Turkish logistics company, Stare Lojistik Enerji Sanayi Ticaret, listed Iran as one of the countries it operates in and that it is located in Igdir, 30 miles from the Iranian-Turkish border. Before they left the United States, two shipments of heavy machinery equipment, scheduled for departure in December 2016, were located and inspected by DOC and DHS at the Port of Savannah in Georgia to verify the contents.[6] At the same time, investigators reviewed e-mail communication between Davidson and the hired shipping agent, Priority Worldwide Services. One of the shipments, valued at $105,666, was ultimately outfitted with a tracking device, "in two separate locations within the contents" of the container.[7] The GPS device allowed the tracking of the shipment to the Port of Mersin in Turkey, and from there to Bazargan, a major border crossing point in Iran, and further to Tehran. According to the complaint, the shipment never went to Stare Lojistik's address as provided in the EEI. The indictment lists a Turkish freight forwarding company as "Unindicted Co-conspirator 1," which is likely Stare Lojistik.[8]

[5] *Affidavit in Support of Application for Arrest Warrant, United States of America v. Aiden Davidson,* p. 1.
[6] Ibid, p. 30.
[7] Ibid, p. 31.
[8] *Indictment: United States of America v. Aiden Davidson and Babazadeh Trading Co,* p.4.

A few months later, the Commerce Department tracked another alleged shipment of heavy machinery equipment from Davidson's company, Golden Gate, to Iran. The shipment was filed in the AES on or about May 3, 2017 and declared to go to Ariyanis Group at Mesihpasa Cad., located in Istanbul, Turkey. The shipment was valued at $13,000 and contained about sixty-three "displacement pumps."[9] According to the complaint, investigators performed a Google search of the alleged recipient but were not able to find a company with the provided name in Turkey. Investigators intervened once again and installed a GPS device "inside a cardboard box that contained the items." They tracked the consignment to Tabriz, Iran, arriving on or about August 1, 2017.[10]

Neither the Ariyanis Group nor the U.S. freight forwarder, Priority Worldwide Services, were named as defendants or co-conspirators in the indictment. Priority Worldwide Services appears to have been involved unwittingly. An online search performed by the Institute found in a publication by the Turkish Ministry of Trade that a company named Ariyanis Foreign Trade Limited Company was cited in a list of businesses with foreign capital investments in Turkey. Ariyanis is listed as a "wholesale trade and commission trade, except of motor vehicles and motorcycles," and the company is listed as based out of Iran.[11]

A parallel DOC investigation into Davidson's past exports found seven additional EEI files for exports from Golden Gate to the same proclaimed recipient of the first tracked shipment, Stare Lojistik. All seven EEIs showed that the shipping agent that acted on Davidson's behalf selected the "No License Required" designation. Golden Gate was registered in New Hampshire as being "involved in the import and export of hydraulic pumps and motors."[12]

The investigation found that Davidson, who was registered as Golden Gate's "manager/member" and agent, appeared to travel to Iran and Turkey frequently, spending several months or weeks there in 2013, 2014, 2015, and 2017.[13] Flight data showed that he departed Iran from Tabriz, where one of the tracked shipments ended up, on at least two occasions. In 2013, Davidson arrived with $15,000 in cash from a trip abroad, which he only declared to U.S. customs during a secondary inspection (an additional interview with Customs and Border Protection officers, referred to by the officer conducting the initial interview at the passport control booth). On subsequent trips, upon returning to the United States, Davidson was referred to secondary inspections several times, but he was always admitted. In 2014, Davidson provided additional contact information and was cleared for entry into the United States. In 2015, U.S. customs personnel found "hydraulic manuals and part numbers, diagrams, and pamphlets," in his luggage, asked "about his shipping activities," and informed him about

[9] *Affidavit in Support of Application for Arrest Warrant, United States of America v. Aiden Davidson,* p.32.
[10] Ibid, p. 32.
[11] Turkish Ministry of Trade, "List of Companies with Foreign Capital in Turkey - As of December 2017," December 2017, https://www.trade.gov.tr/fdi/statistics
[12] *Affidavit in Support of Application for Arrest Warrant, United States of America v. Aiden Davidson,* p. 7.
[13] Ibid.

the Iran embargo.[14] In 2017, he was asked again if he was conducting any business in Iran, which he repeatedly denied.

Search warrants granted in 2017 and 2018 for Davidson's Google e-mail (G-mail) accounts revealed three e-mails sent from Davidson's account in June and July 2013, which appeared to be inquiries for different items for the "'Iran market.'"[15] In one inquiry, Davidson suggested an option to "send out wire transfer through Dubai or HK [Hong Kong]." Davidson's G-mail accounts further revealed communication with his shipping agent, Priority Worldwide Services, where he discussed a shipment to Mersin, Turkey, in April 2015. The communication was forwarded by Davidson to another e-mail address, associated with Babazadeh Trading. In March 2018, the investigation found that Babazadeh Trading sells hydraulic pumps, related accessories and tools, among others, including U.S.-origin items, on their website.

Further investigation of Davidson's e-mail accounts showed he exchanged approximately 2,775 e-mails with the Iranian trading company using different e-mail addresses from January 2013 to April 2018. Many e-mails contained pricing, shipping, and payment details for the nine shipments supposedly destined for Turkey. The investigators further found photographs on the Iranian company's website of items carrying National Stock Numbers (NSNs), which are unique identifiers in the supply chain of the U.S. military. The items were then tied to purchases Davidson made from a liquidity services marketplace for Department of Defense surplus items. The investigation showed that Davidson also purchased industrial parts from Canada on at least two occasions in November and December 2015.

The Scheme

Between 2013 and 2017, on behalf of Babazadeh Trading, a hydraulic pump and related equipment online reseller located in Tehran, Aiden Davidson allegedly used his U.S-registered company, Golden Gate International, LLC, to procure U.S. goods, and send them to Stare Lojistik Enerji Sanayi Tricaret (Stare Lojistik), a freight forwarder and possible front company for Babazadeh Trading located in Igdir, Turkey, which would transship the goods to Tehran. Davidson used an apparently unknowing U.S.-based freight forwarder, Priority World Services, to ship the items to Turkey. Between 2013 and 2017, Davidson, through his company, allegedly received wire transfers from Stare Lojistik and other foreign entities totaling more than $1,000,000, and used these funds to purchase additional items and arrange their shipment to Iran.[16] The goods included machinery parts, hydraulic pumps, electric motors, valves, caterpillar engines and parts, amongst other items. It is unclear how the goods were transported from Mersin to Tehran, or how the goods, which should have been marked as U.S.-origin, by-passed Turkish customs agents. However, Turkey is not known to be vigilant over the nature of items crossing its borders with Iran.

[14] *Affidavit in Support of Application for Arrest Warrant, United States of America v. Aiden Davidson,* p.9.
[15] Ibid, p.12.
[16] *Indictment: United States of America v. Aiden Davidson and Babazadeh Trading Co*., p.6.

Alleged Shipments made prior to insertion of GPS tracking

The first EEI was allegedly filed by Priority Worldwide Services using instructions from Davidson, on or about March 10, 2014. The items were described as "motors, pumps, tools, and other miscellaneous items," and valued at about $130,488.[17] On March 17, 2014, Davidson sent an e-mail to Babazadeh Trading in Tehran notifying them of the shipment and attaching the invoice and a bill of lading. The container number on the bill of lading matched the number in the EEI. Davidson and Babazadeh discussed pricing about a month prior to the exports, between about February 1, 2014 and February 26, 2014. The "final balance" Davidson sent to Babazadeh included a charge for water pumps ($22,000), 15 days of labor ($2,055), "Volvo plus shipping" ($20,125), and a "Tennessee deal balance" ($11,650).[18] It further listed shipment costs as including: "Shipping of 11 eaton big pump from residential to commercial address (no price given)"; "shipping charge for two 40 feet container to Turkey each $3,650" ($7,300); "pallet and box charges" ($430 – 490); and "charge for 2 containers Tennessee deal" ($1,400 – 2,000).[19]

The second and third EEIs were filed on or about March 14, 2014 and on or about August 14, 2014. The items were valued at about $144,625 and $166,000 and were "described as equipment such as engines and pumps" and "equipment such as machinery parts, motors, and other miscellaneous items," respectively.[20] For the former, Davidson allegedly sent an e-mail on March 17, 2014 to Babazadeh Trading in Tehran notifying them of the shipment, again attaching the invoice and bill of lading. Again, pricing was discussed prior to shipment, but no details were included in the complaint. For the third shipment, Davidson allegedly sent a bill of lading to Babazadeh Trading on October 16, 2014. Pricing was discussed between April and May 2014, when Davidson allegedly sent several invoices to Babazadeh, which appeared to be invoices from Davidson's purchases of DOD surplus items, listed as "pumps, valves and motors," and purchased from a company named Surplus Acquisition Venture DBA, Your Direct Source for U.S. Government Surplus.[21]

The fourth and fifth EEIs were filed on or about September 5, 2014, and on or about September 25, 2014. The items, also apparently including DOD surplus goods, were valued at about $173,450 and $42,500 and "described as equipment such as machinery parts and pumps," and "machinery parts, pumps, and motors" respectively.[22] For the fourth shipment, Davidson allegedly sent a bill of lading to Babazadeh on or about December 8, 2014, and a corrected bill of lading on or about December 16, 2014. For both shipments, pricing was discussed prior to the alleged export and included invoices from the same government surplus provider, Surplus Acquisition Venture DBA, "Your Direct Source for U.S. Government Surplus." For alleged shipment four, some items were specified and included brand names, such as "76 PCS Rexroth

[17] *Affidavit in Support of Application for Arrest Warrant, United States of America v. Aiden Davidson,* p. 18.
[18] Ibid, p. 19.
[19] Ibid.
[20] Ibid, p. 20-21.
[21] Ibid, p. 22.
[22] Ibid, p. 25.

Valve 3 Different Lot," and "6PCS Eaton Rotating 3 Different Lot," while the complaint in its summary of invoices and quotes for alleged shipment five generally states "valves, motors and pumps" and "engines."[23]

The sixth EEI was filed on or about April 30, 2015. The alleged export was valued at about $80,000 and "described as equipment such as machinery parts and pumps."[24] According to the complaint, multiple commodities and their prices were discussed prior to the export, which "included pumps and valves."[25] Davidson sent a "direct container line document" to Babazadeh on May 14, 2015, which listed the container number.

The seventh, and apparently last EEI before the GPS tracking was inserted into the shipments, was filed on or about May 7, 2015. It valued the shipment, "described as machinery parts and pumps," at $100,000. Davidson received a "direct container line document" from Priority Worldwide Services, which he forwarded to himself and then sent to Babazadeh on or about May 29, 2015, in an apparent effort to strictly separate the e-mail addresses used for the two. Again, Davidson had "discussed pricing for multiple commodities." He sent a price list of "pieces of thirty one separate items" on or about April 13, 2015, using the subject line "'Anderson eBay items bottom price $59,665'."[26]

Case 10.2: Small Front Companies in Europe Broker Illicit Transshipments of U.S. Aircraft Parts to Iran[27]

A father and son by the name of McGuinn, operating from Ireland and with minimal resources, were allegedly able to run a front company that illegally funneled millions of dollars' worth of U.S. aircraft parts into Iran. Items were allegedly shipped through trading companies and freight forwarders in third-party countries, and onward to Iran and possibly other countries. In one instance, when a U.S. supplier was unwilling to export their products to the Irish company without U.S government authorization, a U.S. freight forwarder facilitated a domestic purchase and then illicitly exported the items to Iran.

Between August 2005 and July 2008, Iran's military aircraft programs allegedly used two Iranian trading companies, Ariasa AG and Onakish Company, to place orders with the Mac Aviation Group of Ireland in order to procure controlled military aircraft parts from the United States (see Figure 10.1).[28] Iran's Aircraft Manufacturing Industrial Company (known by the Persian

[23] Ibid.

[24] Ibid, p. 26.

[25] Ibid.

[26] Ibid, p. 28.

[27] An earlier version of this case study is included in Albright, Paul Brannan, and Scheel (Stricker), "Iran's Procurement of U.S. Military Aircraft Parts: Two Case Studies in Illicit Trade," *Institute for Science and International Security,* May 21, 2009, https://isis-online.org/uploads/isis-reports/documents/Iran_Aircraft_Procurement.pdf

[28] Special Agent David Poole, *U.S. Government Affidavit in Support of Criminal Complaint and Arrest Warrant*, *Hossein Ali Khoshnevisrad*, August 1, 2008, U.S. District Court for the District of Columbia, *Information, United States of America v. Hossein Ali Khoshnevisrad, July 1, 2009*; U.S. District Court for the District of Columbia,

acronym “HESA”) and Iran Aircraft Industries (IACI) allegedly paid Ariasa of Tehran and Onakish of Kish Island to place orders with Mac Aviation Group of Drumcliffe, County Sligo, which would buy the equipment from the United States and ship it through trading companies in Dubai or freight forwarders in Malaysia in order to hide the fact that the end-user was Iran (Figure 10.2). On one occasion, Mac Aviation also procured items directly for Iran Aircraft Industries. Mac Aviation allegedly facilitated payment for the procurements using funds transferred by Iran through complex transaction routes designed to hide their origin.

In September 2008, the U.S. Treasury Department designated HESA a sanctioned entity because of its affiliation with the Iranian Revolutionary Guard Corps (IRGC) and divisions of the Iranian military establishment involved in illicit procurement for Iran’s nuclear or ballistic missile programs. HESA, which is located in Esfahan, is under the umbrella of Iran Aviation Industries Organization (IAIO), which controls Iran’s military aviation projects. The equipment sought by Iran in this case was helicopter aircraft engines, aircraft vanes and bolts, and military cameras. Unlike many cases involving buyers working to purchase items illicitly from inside a procuring state, the manager of Ariasa, Hossein Ali Khoshnevisrad, an Iranian national, was arrested in March 2009 by authorities while on a layover at a U.S. airport.[29] In July 2008, Mac Aviation, its owner, and two employees (one of which turned out to be an alias) were indicted on U.S. charges of facilitating illicit purchases of controlled military aircraft equipment for Iran.[30] Two years later, a U.S. superseding indictment charged Mac Aviation et al. on 27 counts, including violation of the Arms Export Control Act, conspiracy, and making false statements.[31]

Alleged Procurements Brokered by Mac Aviation

Between November 2006 and December 2007, Ariasa and Mac Aviation Group allegedly procured from the Rolls Royce Corporation in Indiana, United States, seventeen helicopter aircraft engines worth $4.7 million, whose end-user was ultimately HESA (see Figure 10.1). HESA or Mac Aviation established an account at the Export Development Bank of Iran in the name of the owner of Mac Aviation, into which money was allegedly deposited as payment for the aircraft parts. Mac Aviation’s owner is believed to have transferred funds from this account to an Irish bank and from there to Rolls Royce’s New York bank account for the purchases. The engines were allegedly shipped in four separate procurements of six, seven, two, and two engines each (see Figure 10.2). Further, according to the latest indictment, Mac Aviation allegedly procured aircraft vanes for Iran from a Connecticut company, aircraft bolts from a Texas company, and canopy panels from a California company. All shipments allegedly involved false end-user declarations and were transshipped via Malaysia or Dubai.

Indictment, United States of America v. Mac Aviation Group et al., July 22, 2008; and U.S. District Court for the District of Columbia, *Indictment, United States of America v. Mac Aviation Group et al.*, July 7, 2010.

[29] U.S. Department of Justice, Press Release, “Iranian Man and his Company Charged in International Scheme to Supply Iran with Sensitive U.S. Technology,” March 16, 2009; Joby Warrick, “Iranian Suspected of Smuggling Weapons for Tehran Jailed in U.S.,” *The Washington Post*, March 17, 2009.

[30] U.S. Department of Justice, Press Release, “Irish Trading Firm and its Officers Charged in Scheme to Supply Iran with Sensitive U.S. Technology,” March 24, 2009.

[31] *Indictment, United States of America v. Mac Aviation Group et al.*, July 7, 2010.

In a communication regarding the first six engines, Mac Aviation explained "delivery to Tehran (Iran) very possible but price – our extra risk, etc. must be fully considered;" it ultimately received a ten percent commission for the first shipment, amounting to $83,400. Ariasa wanted three engines, but Mac Aviation allegedly procured six total engines in order to offer an extra sale.

Mac Aviation did not provide Rolls Royce with legitimate end-user information for the six engines, allegedly stating that the engines would not be sold right away and were intended for "MacGroup usage." The owner of Mac Aviation reportedly told Ariasa that the ordered aircraft engines would be shipped to Kuala Lumpur, Malaysia. New York Express freight forwarding shipped the six engines to "Mac Aviation Group, KS Global Logistics, Selangor Darul Ehsan, Malaysia." Selangor is a Malaysian state encircling Kuala Lumpur, and Mac Aviation appeared to have had a warehouse in Selangor from which the engines would be diverted to Iran. An internet search revealed that KS Global Logistics is a "freight, transportation, and logistics" service. The e-mails also allegedly warned "Note—Aviation/equipt embargo very very strong right now on Iran extreme vigilance worldwide in place."

For the next set of seven engines, a representative of Mac Aviation was invited to travel to Kish Island, Iran to discuss the deal and "new projects." The cost for the six engines would be $1,483,020, and when placing its order with Rolls Royce, Mac Aviation allegedly specified the end-user of the equipment as "Penerbit Kemas Sdn. Bhd," which was either a company or freight forwarding location in Malaysia. Later that month, one of the defendants allegedly met with a Rolls Royce representative at an air show in Paris. The representative informed Mac Aviation that Rolls Royce would not be able to sell the six engines until appropriate end-user information was given for the last six engines. The representative also inquired as to why Mac Aviation had provided a "Malaysian publishing company" as the end-user for the new sale. The address of this company was also that of a freight forwarding location. Mac Aviation's representatives allegedly responded to Rolls Royce that the Malaysian Ministry of Defense was the true end-user for the engines and a Malaysian broker had been acting on its behalf.

Mac Aviation kept changing the end-user information it provided, allegedly notifying Rolls Royce that it would eventually be selling or renting these engines to "operations" in Malaysia, Indonesia, Bangladesh, Romania, Nigeria, Ghana, Mauritania, and perhaps Singapore and Libya. It also allegedly assured the company that it would not sell to any governments or military organizations. Despite the inconsistencies, Rolls Royce shipped in two different shipments from its New York freight forwarding company the seven engines, with the packages addressed to Penerbit Kemas Sdn. Bhd., the "publishing company" identified by Rolls Royce (Figure 10.2). Shortly after, Mac Aviation allegedly transferred to Rolls Royce a payment of $1,904,564 for the engine sale after it received funds from HESA.

The shipments for the last four engines followed the same scheme, but the scheme for the aircraft vanes and bolts differed slightly. Mac Aviation allegedly told the supplier that the final destination for the vanes was Belgium. It is not clear how the vanes were diverted from

Belgium to Malaysia, but an invoice Mac Aviation allegedly issued directly to IACI referenced an Air Waybill, which allegedly showed that the items were to be transferred to Iran via a flight from the international airport of Kuala Lumpur, Malaysia, bound for Tehran/Mehrabad International Airport (Figure 10.2).

The bolts were purchased by Mac Aviation from a U.S. company in Texas (Figure 10.1) and shipped through an unidentified Dubai trading company to Onakish Co., the above-discussed Iranian company purchasing on behalf of the state's military aircraft programs (Figure 10.2). Mac Aviation allegedly told the Dubai trading company, which was also paying for the items, that it would only accept payment from a Dubai bank, and allegedly reminded them that "any payment from Iran will not be accepted by European banks." Delivery details allegedly noted the need to omit the name of the Dubai trading company from shipping documents, due to the extra scrutiny applied to U.S. exports going to the UAE.

The superseding indictment added two charges for Mac Aviation's alleged role in procuring and exporting U.S.-origin F-5 fighter aircraft parts, which is a violation of the Arms Export Control Act. Specifically, in 2005, the defendants allegedly exported "canopy panels, designed for the F-5 fighter aircraft, valued at approximately $44,500," to Sasadja Moavanate Bazargani in Tehran, which acted on behalf of HESA (Figure 10.2). The new charges relating to this alleged procurement would add another possible ten years in prison for the father and son, if they are ever tried in the United States and found guilty.[32]

The alleged procurement of the canopy panels proved difficult but was ultimately successful. The U.S. supplier, Commerce Overseas Corp., reportedly declined the order repeatedly due to insufficient end-user information and requests by Mac Aviation to export the items without an export license. At least one freight forwarder also declined to assist the export without an export license.[33] According to a 2010 *Bloomberg* report, Mac Aviation finally found a U.S. freight forwarder to pose as the recipient so that a license would not be needed. Upon receipt, the freight forwarder, identified as ABL Freight of California, allegedly removed the invoices, and, according to *Bloomberg,* fabricated documents that described the canopy panels as "plastic panels."[34] In February 2006, the freight forwarder allegedly shipped the canopy panels to a Free Commercial Zone in Kuala Lumpur, without the required U.S. export license, from where they were transferred to Tehran (Figure 10.2).[35] A price quote Mac Aviation sent directly to HESA was allegedly twice the amount for what Mac Aviation had paid for the parts.

---

[32] U.S. Department of Justice, Press Release, "New Charges Filed Against Irish Trading Firm for Exporting U.S. Military Items to Iran," July 7, 2010, https://www.justice.gov/opa/pr/new-charges-filed-against-irish-trading-firm-exporting-us-military-items-iran

[33] *Indictment, United States of America v. Mac Aviation Group et al.*, July 7, 2010.

[34] Justin Blum, "American Iran Embargo Thwarted When Smugglers Ship Made-In-USA," *Bloomberg*, October 21, 2010, https://www.bloomberg.com/news/articles/2010-10-21/american-iran-embargo-undermined-as-smugglers-show-way-to-ship-made-in-usa

[35] *Indictment, United States of America v. Mac Aviation Group et al.*, July 7, 2010, p. 28.

Bloomberg uncovered in October 2010 that Mac Aviation also allegedly attempted to procure laser cutting machines for Iran, which have potential missile development applications and can be used for "chemical weapon detection kits."[36] At the time of this writing, the defendants were still at large in Ireland and continued to deny all charges.

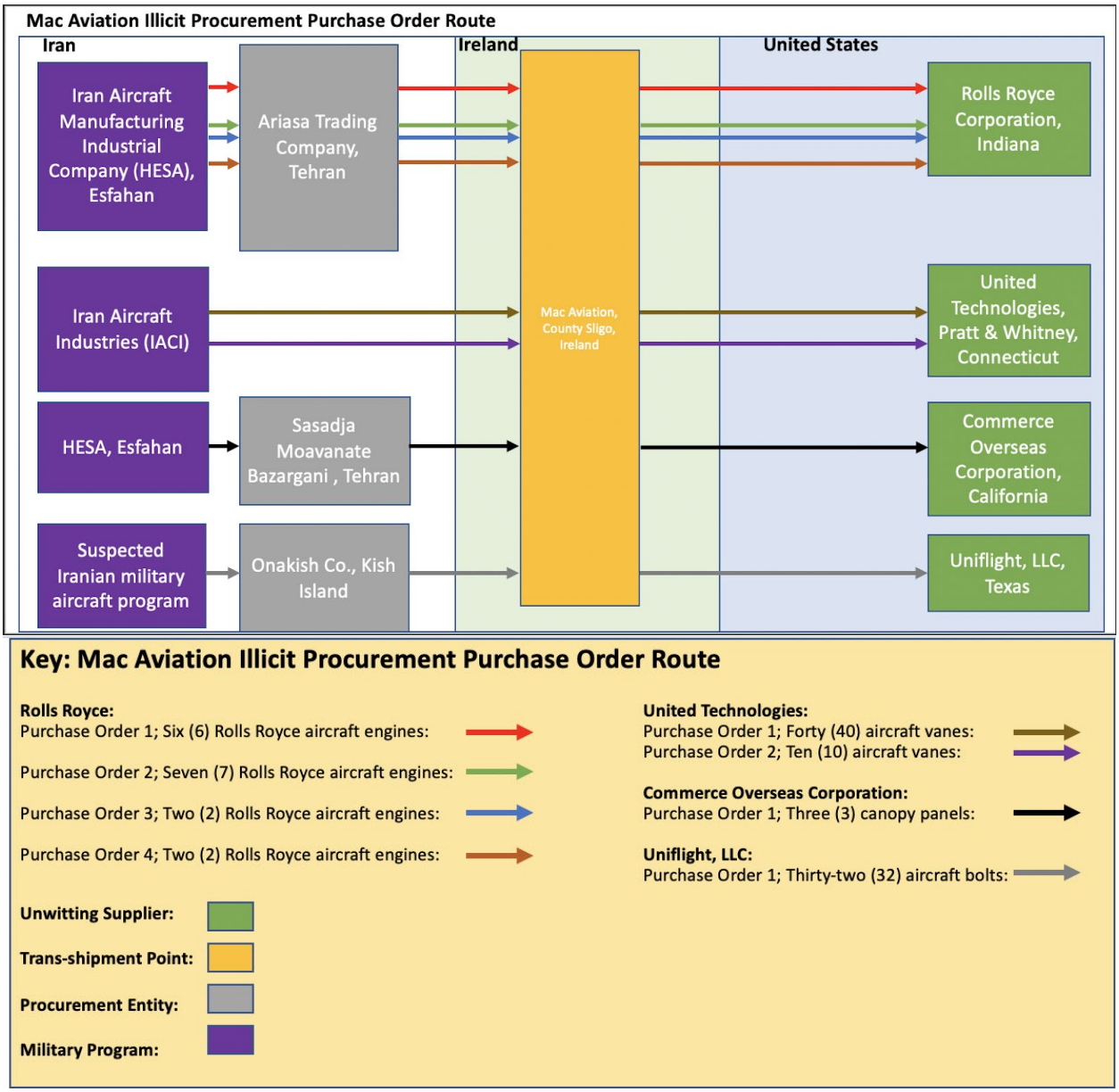


Figure 10.1. Procurement routes for the various exports allegedly brokered by Mac Aviation.

[36] "American Iran Embargo Thwarted When Smugglers Ship Made-In-USA."

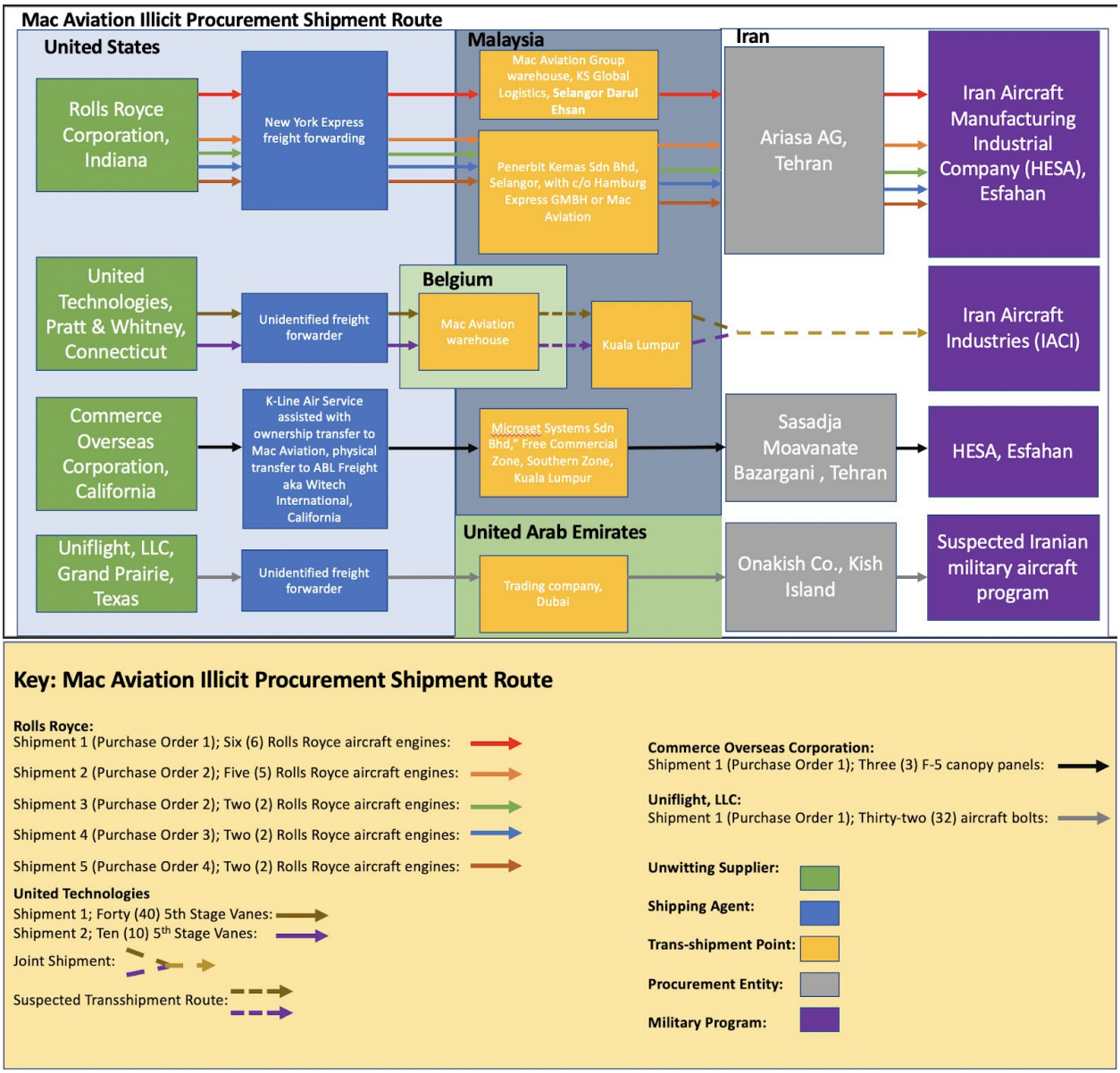


Figure 10.2. Shipment routes allegedly used by Mac Aviation for the illicit exports.

A Small Front Company with a Long History of Suspicious Sales

Ireland's *Sunday Times* found in an investigation that Rolls Royce and other major suppliers were apparently fooled by Mac Aviation's large and global appearance, when in reality, just the father and his son were running the company from their small home in a rural part of western Ireland. Using limited resources, including a simple fax machine, two-line phone, and computer, they generated large profits through carefully procuring equipment using a variety of fronts. The company created fictitious employees to lend an appearance to its customers that it was a large operation with many employees. For example, an employee, "Sean Byrne," was later determined to be fictitious despite his inclusion in the 2008 U.S. indictment. When an

official from Rolls Royce visited the company, he was reportedly speechless because he had thought it was a global operation that employed hundreds of people.[37]

The father, Thomas McGuinn, was arrested in 1994 for illegally selling U.S.-made night vision goggles to Iran.[38] The conviction apparently did not deter him from continuing his alleged, illicit and lucrative business in Ireland, and, regrettably, did not lead to sufficient and coordinated U.S. company or government vigilance. According to *The Sunday Times*, by 2010 alone, the company had generated as much as €85 million worth of deals with Iran.[39]

The case remains open as of this writing, and it is unclear what action Irish authorities have taken to address the McGuinns' activities. Mac Aviation settled a court case with Ireland's Criminal Assets Bureau in 2010 and agreed to pay 1.5 million Euros.[40] Extradition of the McGuinns from Ireland to stand trial for their alleged violations of U.S. law is not certain because the charges are not covered in Ireland's extradition treaty with the United States. According to Irish tabloid reports, Thomas McGuinn appeared on Interpol's "Red Notice for wanted persons" list in 2014, but a search conducted by the Institute in 2019 found no such listing.[41]

A Broker and a Complicit Freight Forwarder in the Netherlands

Ariasa also allegedly procured military aircraft cameras from the United States, not using Mac Aviation, but a Dutch company as an intermediary (Figure 10.3).[42] In 2006, the manager of Ariasa allegedly contacted a company in the Netherlands that supplied aviation equipment and asked it to procure from a Pennsylvania firm ten aerial panorama cameras and one military camera that could be used on the F-4-E Phantom fighter bomber, currently in use by Iran's air force. Ariasa allegedly told the Dutch company to use the Netherlands as an end destination on customs documents, and to specify the cameras would be used by a "geographical university to lern them (sic) how to film from the air."[43] According to legal documents, the camera order was allegedly shipped in August 2006 from the Netherlands to Tehran aboard an Iran Air flight (Figure 10.3).

The Dutch company, Aviation Services International B.V. (ASI), its director, Robert Kraaipoel, and his son and sales manager, Niels Kraaipoel, were charged in September 2009 in the U.S.

---

[37] John Mooney, "U.S. Links Sligo to €40m Iran Arms Web," *The Sunday Times* of Ireland, October 18, 2009. http://www.timesonline.co.uk/tol/news/world/ireland/article6879300.ece

[38] Ibid.

[39] John Mooney, "Sligo Firm 'Made €85m Worth of Illegal Exports'," *The Sunday Times* of Ireland, November 7, 2010, https://www.thetimes.co.uk/article/sligo-firm-made-euro85m-worth-of-illegal-exports-fmvkd8n3z9h

[40] Daniel O'Carroll, "Irish aviation company settles with CAB over Iran row," *Irish Central*, July 27, 2010, https://www.irishcentral.com/news/irish-aviation-company-settles-with-cab-over-iran-row-99334674-237707151

[41] See: Ailbhe Jordan, "Irish Sunday Mirror Investigates: 12 of the world's most-wanted criminal suspects who all come from Ireland," *Irish Mirror*, January 11, 2015, https://www.irishmirror.ie/news/irish-news/crime/irish-sunday-mirror-investigates-12-4959731

[42] *U.S. Government Affidavit in Support of Criminal Complaint and Arrest Warrant*, *Hossein Ali Khoshnevisrad*.

[43] Ibid, p.12.

District Court for the District of Columbia with conspiracy to export to an embargoed country.[44] The father-and-son team pleaded guilty shortly after and asked for mitigating sentences because of their extensive cooperation. The Information document in the case showed that Ariasa was not their only Iranian customer, and the cameras were not their only illicit sale (see Figure 10.4). Rather, ASI procured goods illicitly for Iran from 2005 to 2007, including electronic communications equipment, and attempted to procure additional goods, including aluminum sheets and rods and polymide film. According to the indictment, the items were transshipped through third party countries including Georgia and Cyprus. After U.S. customs interdicted a January 2007 shipment, the illicit activities allegedly continued under a new company name, Delta Logistics B.V., at least until about October 2007 or possibly longer, when the U.S. government placed a trade block, in the form of a Temporary Denial Order (TDO) for all U.S. exports by the company.

According to legal documents, the defendants provided the U.S. government with extensive information on "their Iranian customers, the Iranian end-users, the freight forwarders in the Netherlands, and their U.S. suppliers."[45] Ulrich Davis, a manager of the Netherlands-based freight forwarder, was apparently complicit in at least one of the Kraaipoel exports, allegedly conducted additional illicit procurements of aircraft parts from a New Jersey company himself, and offered Kraaipoel assistance in evading the TDO after it was instituted.[46] He was arrested at a U.S. airport in August 2011 and sentenced to six months in prison. According to the criminal complaint against Davis, the freight forwarder assisted in "neutralizing" the packages before shipping them from the Netherlands to Iran, by removing invoices and packing lists, and ordered their transport provider to do the same. Davis allegedly organized shipments through an affiliated New York freight forwarder from the United States to the Netherlands, and onward to Iran.

Kraaipoels' cooperation and insider information, claimed the U.S. government, led to "a change in how freight forwarders conducted business, thereby making more difficult to transship items to Iran."[47]

[44] United States District Court for the District of Columbia, *Superseding Information, United States of America v. Aviation Services International B.V. et al,* September 18, 2009.
[45] United States District Court for the District of Columbia, *Government's Motion for Downward Departure and Sentencing Memorandum, United States of America v. Robert Kraaipoel*, June 5, 2012.
[46] Special Agent David Poole, United States District Court of District of New Jersey, *Criminal Complaint, United States v. Ulrich Davis*, August 5, 2011.
[47] *Government's Motion for Downward Departure and Sentencing Memorandum, United States of America v. Robert Kraaipoel*.

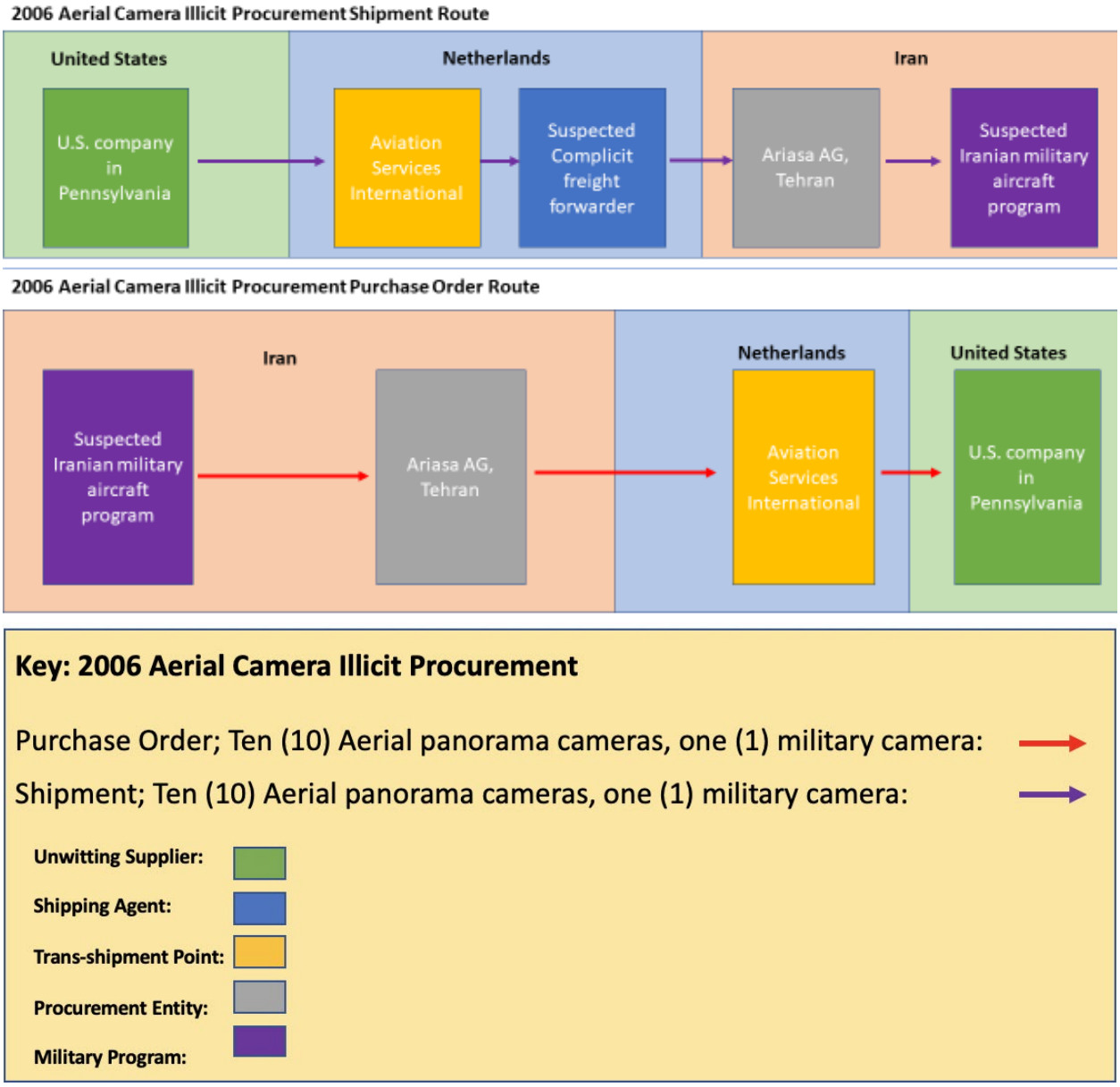


Figure 10.3. Shipment and procurement routes for the military cameras.

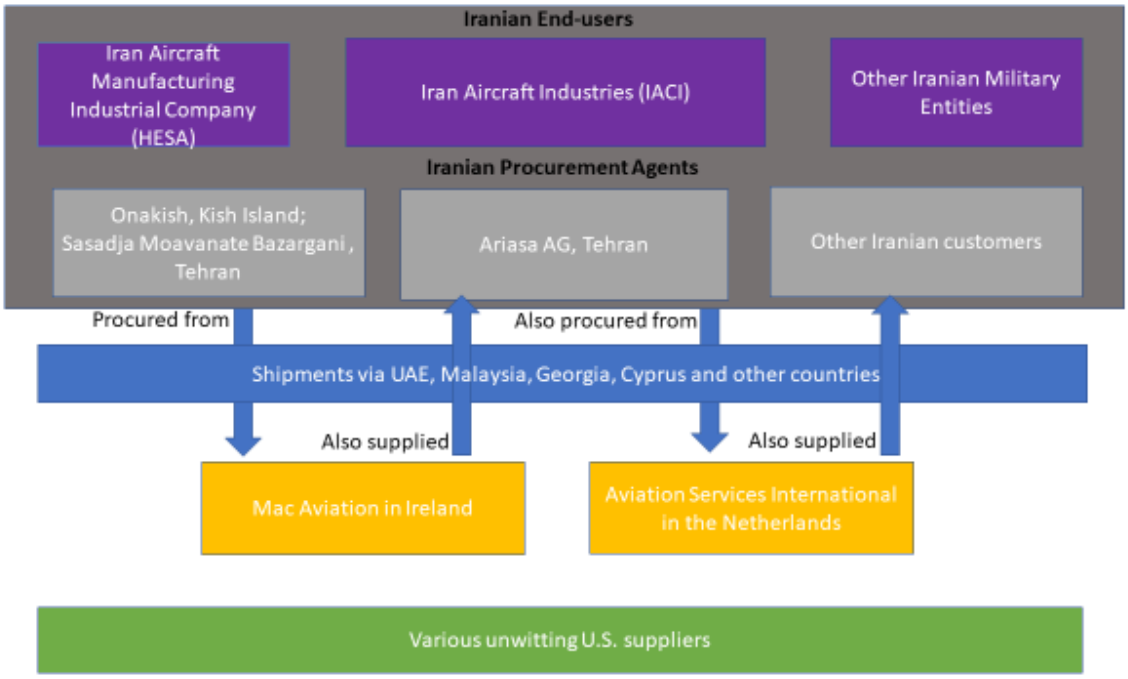


Figure 10.4. The McGuinns and the Kraaipoels allegedly worked with the same Iranian procurement agent, Ariasa. However, they also worked with other Iranian agents, widening the illicit procurement network and causing the export of aircraft parts and other items worth millions of dollars to Iranian military end-users.

Case 10.3: Chinese Nationals Residing in the United States Use Fraudulent U.S. Driver's Licenses to Purchase and Export Night Vision Goggle Equipment to China

On July 25, 2019, the Department of Justice released an Information document alleging that between April 2017 and October 2018, Yuankai Yang, along with two other unnamed, unindicted Chinese nationals, sought to purchase domestically and export illegally many types of controlled night vision goggle (NVG) equipment and accessories from a supplier located in Texas, to China.[48] Yang, a permanent resident of Williamstown, New Jersey since 2015, was charged with one count of conspiracy to violate the Arms Export Control Act and one count of conspiracy to commit money laundering. The case was being prosecuted in the U.S. District Court for the District of New Jersey, Camden Court. According to an analysis of available public records, Yang has pleaded guilty to both charges and is scheduled to be sentenced on October 9, 2019.[49]

[48] United States District Court in the District of New Jersey, *Information, United States of America v. Yuankai Yang*, 19 CR 528 (2019), Filed July 25, 2019. Available at https://www.pacer.gov

[49] Jim Walsh, "Williamstown Woman Admits Guilt to Night-Vision Smuggling Scheme," *The Courier Post*, July 29, 2019, https://www.courierpostonline.com/story/news/2019/07/29/yuankai-yang-williamstown-nj-smuggled-night-vision-goggles-defense-items-china/1851624001/

The Scheme

Between April 2017 and October 2018, Yang and her co-conspirators sought to purchase night vison goggle equipment from a U.S. NVG supplier and illegally export it to China. The two Chinese co-conspirators allegedly directed Yang to purchase specific types of NVG from the U.S. based supplier(s) and transferred money through U.S. financial institutions to Yang to pay for the purchase.[50] Between October 23, 2015, and April 30, 2018, Yang received $208,289 via wire transfers from banks located in China, to her bank account in the United States, which was in the District of New Jersey. Yang shipped the NVG equipment, which requires U.S. State Department authorization for exports, to China, via mail or commercial carrier and without a license. As part of the scheme, Yang recruited U.S. citizens to provide driver's licenses to certified NVG distributors/suppliers to support her false claim that the sale was domestic and that the end-user of the goods was a U.S. citizen located inside the United Sates. The conspirators further provided falsified documentation/identification, aliases, and deliberately submitted incorrect end-user statements to the supplier of NVG's in order to disguise the true purchaser and the end destination of the controlled goods.

Yang admitted to having purchased NVG equipment and accessories controlled under the Arms Export Control Act and the International Traffic in Arms Regulations (ITAR), listed on the United States Munitions List (USML). She admitted to exporting the items without the required export license and approval by the U.S. State Department Directorate of Defense Trade Controls (DDTC). Neither Yang nor her co-conspirators applied for or received an export license authorizing the export of NVG equipment or accessories to China.

Posing as U.S. Citizen on the Internet to Cause a Purported Domestic Sale

In April 2018, Yang and her co-conspirators in China attempted to procure NVG equipment and accessories using at least one fraudulent California driver's license. One unindicted Chinese national, using the alias "David Guan," via the internet, ordered two DVS-110-22Gs from Nivisys for $10,294, to be shipped to a global courier company in Portland, Oregon. The DVS-110-22G is a submersible "state-of-the-art 2nd or 3rd Generation hand-held night vision viewer... and can be submerged to 20 meters underwater."[51] On April 18, 2018, the unindicted Chinese national provided Nivisys an "End User Agreement," and a copy of the fake driver's license. On May 2, 2018, Yang arranged for a wire transfer of $10,332.22 from Bank of America to the bank account of Nivisys as payment for the DVS-110-22Gs.

[50] The supplier company was likely Nivisys Industries LLC, a manufacturer and designer of night vision goggles equipment and accessories, based in El Paso, Texas. Nivisys is the only manufacturer of many of the defense articles procured by Yang and the conspirators. When accessing Nivisys's website, the user is prompted by a pop-up window to acknowledge that NVG equipment and accessories are subject to U.S. export controls and requires an export license approved by the Department of Treasury in order to export.

[51] "DVS-110, Diver Night Vision System," *Nivisys Industries LLC*, September 2019, http://www.nivisys.com/en/products/night_vision_systems/dvs_100/

From Portland, Oregon, unbeknown to Nivisys, the two DVS-110-22G NVG's were shipped to Shanghai, China. It is unclear in the Information how the goods passed through customs without the proper export approval.

Case 10.4: Iranian Agents Residing in the United States Illicitly Export Domestically-Purchased U.S. Military Goods [52]

From 2006 until mid-2007, Hassan Saied Keshari and Traian Bujduveanu, both naturalized U.S. citizens and residing in the United States, engaged in six acts of illicit trade to provide Iran with controlled U.S. military aircraft parts.[53] In this scheme, two unidentified individuals located in Iran placed orders for U.S. attack aircraft equipment through the California company operated by Keshari, called Kesh Air International Corporation. Keshari, originally from Iran, procured equipment from U.S. manufacturers through Bujduveanu's Florida-based company, Orion Aviation Corporation (Bujduveanu is Romanian by birth). Together, Keshari and Bujduveanu arranged shipment of the equipment to Dubai via a freight forwarder, where it was then diverted to Iran. In June 2008, Keshari and Bujduveanu were arrested by U.S. authorities and both pleaded guilty to illicit trading activities in 2009. They were sentenced to seventeen months and thirty-five months in prison, respectively.[54, 55]

The Iranians directing procurement orders to Keshari were likely either officials at an Iranian military aircraft program or worked for a company responsible for procurement on behalf of the aircraft program. They would send Requests for Quotes (RFQs) for desired equipment to Keshari, who in turn would ask Orion Aviation to obtain price quotes directly from U.S. manufacturers. After communicating with the two Iranians, Keshari and Kesh Air transferred funds to Orion Aviation to pay for the purchases.

The military aircraft equipment sought by Iran were spare parts for its AH-1 Cobra attack helicopters, F-14 fighter jets, and CH-53A military helicopters. At the time, the items were controlled for export by DDTC under the Munitions List. Any such export was illegal to Iran. Keshari and Bujduveanu did not seek export licenses for the equipment they sent to Iran.

---

[52] See for the full version of this case study: David Albright, Paul Brannan, and Andrea Scheel (Stricker), "Iran's Procurement of U.S. Military Aircraft Parts: Two Case Studies in Illicit Trade," *Institute for Science and International Security,* May 21, 2009, https://isis-online.org/uploads/isis-reports/documents/Iran_Aircraft_Procurement.pdf

[53] U.S. District Court for the Southern District of Florida, *Indictment, United States of America vs. Hassan Saied Keshari, Traian Bujduveanu, Kesh Air International Corp., and Orion Aviation Corp.,* Case No. 08-20612-CRSEITZ/O'SULLIVAN, July 3, 2008, released January 26, 2009.

[54] "Iranian-American Sentenced in Iran Smuggling Plot," Reuters. May 14, 2009, https://www.rferl.org/a/IranianAmerican_Sentenced_In_Iran_Smuggling_Plot/1732260.html

[55] U.S. Department of Justice, Press Release, "Defendant Sentenced in Conspiracy to Export Military Aircraft Parts to Iran," June 11, 2009, https://www.justice.gov/opa/pr/defendant-sentenced-conspiracy-export-military-aircraft-parts-iran

Illicit Shipments

The order and shipment routes for the six exports are visualized in Figures 10.5 and 10.6. When shipping the first order, Bujduveanu declared the contents of the shipment to be "commercial aircraft parts" worth $900. These aircraft parts were actually worth more than $4,000 and should have been declared military in application, according to the U.S. indictment against Keshari, Bujduveanu, and their companies. At a declared value of $4,000, Bujduveanu would have been required to file what was at that time called a Shipper's Export Declaration, now Electronic Export Information, mandatory for all international shipments exceeding a value of $2,500. For all arranged shipments, Keshari sent e-mail notifications to the two Iranian individuals located in Iran with shipping information for the equipment that was en route to Dubai.

Keshari, Bujduveanu, Kesh Air International Corporation, and Orion Aviation Corporation stood to forfeit any parts and equipment seized by the U.S. government from their homes and companies in June 2008 at the time of their arrest. Aircraft assemblies and parts were seized from the residence of Bujduveanu. They also stood to forfeit proceeds of the equipment sold to Iran. Over forty thousand dollars was seized from the home and bank account of Bujduveanu, while almost sixty thousand dollars was seized from the bank account of Keshari.[56]

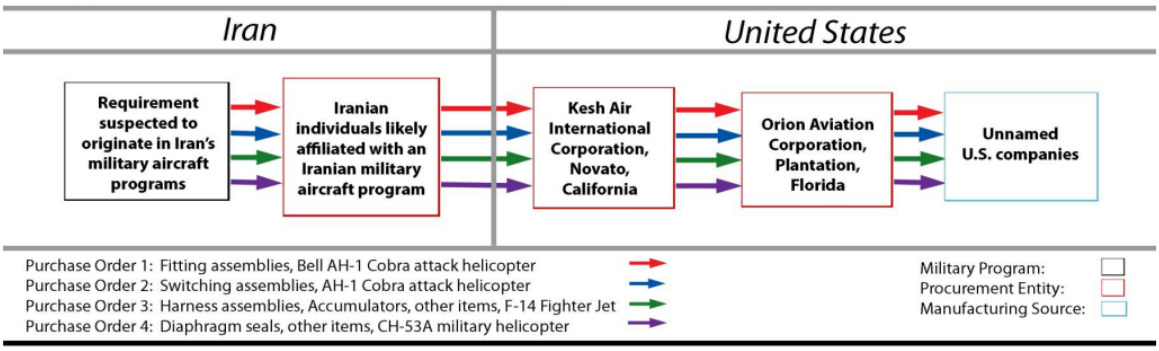


Figure 10.5. Iran's procurement of controlled military aircraft equipment: Order route.

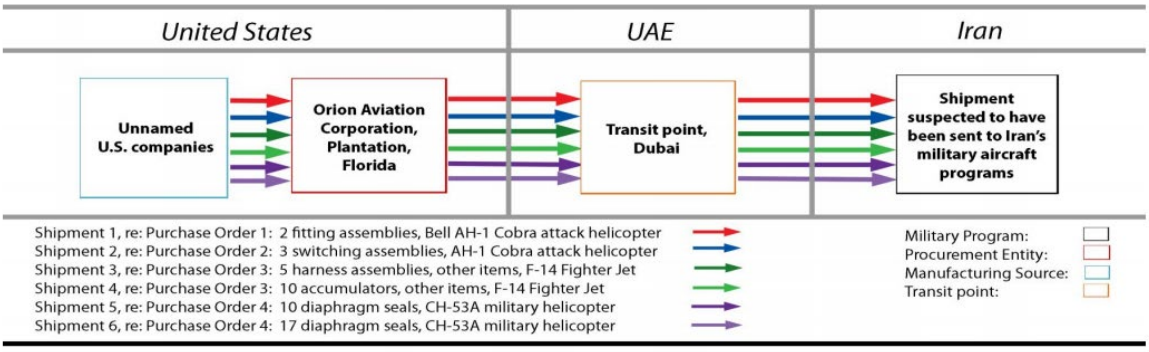


Figure 10.6. Iran's procurement of controlled military aircraft equipment: Shipping route.

[56] *Plea Agreement, United States of America vs. Traian Bujduveanu.*

Annex to Section III: Key Stakeholders

Numerous parties can be involved in a shipment, including maritime carriers, airlines, air cargo services, e-commerce, free port operators, fast parcel services, shipping lines, trains, and trucks. The following annex describes the roles of these actors.

Carriers, or Transport Service Providers (TSP), (both private and public), have limited oversight over the goods they carry, and often lack the legal authority to open a sealed package or enter a locked container to verify its contents. However, they do require a set of paperwork and documentation (a contract, at least) and can be held liable for knowingly assisting in the unlicensed export of controlled goods or the export of goods to a sanctioned entity. Often, but especially for transit and transshipment through countries where the exporter does not operate, it is the carrier that submits the customs declaration, often prior to arrival.[1] The carrier can also provide customs with additional, non-required information that it can use to make a risk-assessment, for example, information drawn from the carrier's electronic information system, if applicable.[2]

The transport provider can use contractual language to introduce a blanket ban on sanctioned activities, and note that the contract can be voided and services will not be provided in such cases. Further, and more directly, the transport provider can make the diversion of goods more difficult and prevent its own shipping capabilities from being used in a diversion by requesting the immediate return of rented equipment, such as shipping containers, upon arrival of the goods at the declared destination. According to a report by the Royal United Services Institute (RUSI), one shipping company with customers in China employs this tactic to prevent its containers from ending up in North Korea.[3]

In the United States, a bill of lading and a commercial invoice for controlled goods need to include a Destination Control Statement "to notify the carrier and all foreign parties that the item can be exported only to certain destinations."[4] Additionally, exporters from the United States must file an Electronic Export Information entry for a licensed export, or any export valued at over $2,500, and this must list the final destination. A freight forwarder, logistics company or customs warehouse is not a legitimate final destination for inclusion on an EEI, and its listing may warrant greater scrutiny by export authorities, and should require caution and suspicion by shippers.

Owners, managers, crew, and port authorities, both for sea and for air traffic, have a personal stake in ensuring the commodities they transport are not illicit. A U.S. Treasury Department

[1] Aaron Dunne, "The Role of Transit and Trans-shipment in Counterproliferation Effort" (Stockholm: Stockholm International Peace Research Institute, *SIPRI Good Practice Guide*, No. 6, September 2016).
[2] "The Role of Transit and Trans-shipment in Counterproliferation Effort," September 2016.
[3] Eli Dall and Tom Keatinge, "Underwriting Proliferation – Sanctions Evasion, Proliferation Finance and the Insurance Industry" (London: Royal United Services Institute, July 2018).
[4] "Common Export Documents," Export.gov, accessed August 14, 2019, https://2016.export.gov/logistics/eg_main_018121.asp

advisory on North Korea's illicit shipping practices lists the risks for masters, crew, ownership, and management when a vessel is associated with or conducts illicit activities. It reminds owners and managers of their ultimate liability for the vessel's activities, and the master's and crew's liability for knowingly making "false claims of registration."[5] It warns that law and sanctions violators can be prosecuted or become subject to OFAC sanctions, and that ships improperly registered can be inspected and boarded anytime. Further, the advisory recommends masters and crews to be wary if "required registry, safety, pollution prevention, and manning certificates do not match or the required Continuous Synopsis Record is not properly maintained."[6] Lastly, documentation submitted to or by the different parties, such as proof of insurance, last ports of call, or cargo declarations, can provide valuable insights to port and other authorities screening for signs of illicit activity.

Freight forwarders and customs brokers arrange the shipment of a good, and may, depending on national laws, assume the same level of responsibility for ensuring the export is lawful as the supplier itself.[7] For example, they may assist with packing the goods and filling out and submitting required export information and documents. They may choose the route, the carrier, the means of transportation, and often remain in charge of the shipment until delivery. In the United States, for example, shipments that require an export license, as well as any shipment valued over $2,500, need to be filed in the U.S. Automated Export System (AES), but suppliers can authorize a company like FedEx to also meet Electronic Export Information requirements.[8] Commerce Department guidance recommends freight forwarders have their own compliance programs, because in the United States, as one of the parties involved in an export transaction, they can always be held accountable to some degree if the export was illicit and they failed to conduct due diligence.[9] Companies, including DHL and FedEx, have been held liable for non-compliance with the EAR, showing that the U.S. government is willing and able to enforce its laws. Further recommendations include applying due diligence, such as being aware of common red flags, building compliance partnerships with exporters, requiring certain documentation be submitted (such as the Destination Control Statement or similar), even when not required by other countries' laws, ensures the maintenance of records as required by U.S.

[5] U.S. Department of Treasury, "Updated Guidance on Addressing North Korea's Illicit Shipping Practices," March 21, 2019, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_vessel_advisory_03212019.pdf

[6] Ibid.

[7] In the United States, the primary responsible parties for export control purposes are the "principal parties in interest" in the transaction, which are usually the U.S. seller and the foreign buyer, but an authorized agent can also be a responsible party. See: U.S. Department of Commerce, "Freight Forwarder Guidance," February 2012, https://bis.doc.gov/index.php/documents/compliance-training/export-management-compliance/620-new-freight-forwarder-guidance/file

[8] See, for example, "FedEx Export AgentFile," Electronic Export Information, FedEx.com, accessed August 21, 2019, https://www.fedex.com/en-us/shipping/electronic-export-information.html#export-agentfile

[9] "Freight Forwarder Guidance."

law. Shippers can also reach out to the Commerce Department for compliance questions, and use Voluntary Self Disclosure programs, if applicable.[10]

As discussed in Chapter 9, in 2019, FedEx filed a formal legal complaint regarding its freight forwarding liability for violations of the EAR. The complaint, filed on June 24, 2019, cited privacy-infringement concerns and illustrated the difficulty for a shipping agent to know the specific contents of packages. Commerce Secretary Wilbur Ross responded in a statement that FedEx had "misinterpreted" the EAR, stating, "'What the regulations simply say is that neither FedEx nor any other common carrier can knowingly carry goods that are in violation of the rules – knowingly.'"[11] On September 10, 2019, the Commerce Department filed a motion to dismiss the case.[12] While a difficult issue for carriers, their often inadvertent participation in illegal exports remains a major challenge.

Customs and other border control agents face their own limitations. The sheer volume of container traffic to clear and inspect is immense, so a key question is how they should prioritize. They spend a considerable amount of effort to determine what level of suspicion warrants detainment or inspection, and leads to a decision to stop and search, potentially seize, and report their findings. The latter can require waiting potentially long periods for feedback from authorities. In some countries, customs authorities can face personal liability for causing a delayed shipment.

Customs agencies, in general, are aware of their role in stopping strategic commodity trafficking. Tip-offs from other agencies and domestic authorities, and entity-based physical inspections, have shown to be key for many successful customs interdictions. Certain indicators also assist this task. For example, according to a UN sanctions investigator quoted by Reuters, there is already "a 50 percent chance that a customs officer will undertake a search," if a ship is Iranian-flagged.[13]

Goods in transit and undergoing transshipment need to be declared to customs as such, aside from tax and duty purposes. Customs declarations and relevant documentation, such as cargo

---

[10] Submitting a Voluntary Self Disclosure allows a party that believes it may have violated U.S. export regulations to provide this information voluntarily to authorities in exchange for consideration of reduced penalties if a violation occurred.

[11] Bruce Leeds, "FedEx vs. Department of Commerce: Compliance Comes in Small Packages," Braumiller Law Group, August 15, 2019, https://www.braumillerlaw.com/fedex-vs-department-of-commerce-compliance-comes-in-small-packages/

[12] Max Garland, "U.S. Department of Commerce Calls for FedEx Lawsuit over Export Rules to be Dismissed," *Memphis Commercial Appeal*, September 11, 2019, https://www.commercialappeal.com/story/money/industries/logistics/2019/09/11/fedex-sues-commerce-department-export-administration-regulations/2290695001/

[13] Jonathan Saul, Parisa Hafezi, and Marianna Parraga, "Flags of Inconvenience: Noose Tightens Around Iranian Shipping," Reuters. July 26, 2019, https://www.reuters.com/article/us-mideast-iran-tanker-flags-insight/flags-of-inconvenience-noose-tightens-around-iranian-shipping-idUSKCN1UL0M8?utm_source=In+Escalation%2C+Iran+Tests+Medium-Range+Missile%2C+U.S.+Official+Says&utm_campaign=eye-on-iran&utm_medium=email

manifests, as well as documents required for transportation, can help authorities identify suspicious or high-risk shipments in transit and undergoing transshipment. Internationally-required transportation documents include a certificate of origin and a dangerous goods declaration, if applicable. For rail and road transport, a consignment note, the CIM or CMR, respectively, is internationally required.[14] For carriage by air, an Air Waybill or an equivalent form of receipt is required, and for sea shipment, a bill of lading is common, which includes a description of the goods and their condition. Types of bills of lading include Inland Bill of Lading, Multimodal Bill of Lading, and 'to order' bills of lading, where the intended consignee is not automatically the new owner of the goods.[15]

A list of international UN-required trade documents can be found in the *United Nations Layout Key for Trade Documents.* States' domestic trading laws may require additional shipping documentation. Further, there are a variety of recommended, standardized, or region-specific documents. A Single Administrative Document is required for trade within the EU.[16] The World Bank keeps track of countries' national documentation requirements as part of its *Ease of Doing Business* database.[17] Common documents accompanying a shipment include an insurance certificate, a charter agreement, a commercial invoice, an Air Way Bill, sea Bill of Lading, a packing list, a dock receipt, and a list of last ports of call.

Bills of lading and invoices have proven especially helpful for investigations and prosecutions of U.S. export control violations. Illicit procurement networks often hide the original documents showing the true goods or the true recipient from vigilant licensing officials, customs officers, and shipping agencies, sometimes providing a falsified version, but search warrants have often been able to recover the originals during investigations. They can provide valuable evidence for indictments and allow authorities to establish the illicit network's strategy, intent, and the relationship between an illicitly-traded good and its true nature or end-users.

Free Trade Zones (FTZs) and other special economic zones present a problem to trade regulation. There is both a global lack of licensing and trained customs authorities enabled to fulfill strong strategic trade control duties in Free Trade Zones and other specially administrated economic zones. One international regulation is found in the Revised Kyoto Convention, specifically in Chapter 2 of Specific Annex D. Recommendation 4 in the chapter states that "customs shall have the right to carry out checks at any time on the goods stored in a free

[14] "UN Layout Key for Trade Documents" 2002.
[15] Ibid.
[16] Ibid.
[17] See, for example, The World Bank, Ease of Doing Business, "Details – Trading across Borders in Afghanistan – Trade Documents," https://www.doingbusiness.org/en/data/exploreeconomies/afghanistan#DB_tab

zone."[18] However, contracting parties to the convention have to accept the recommendations in the Annex, and only 21 states have accepted Recommendation 4 as of 2018.[19]

Open ship registries that allow foreign-owned vessels to fly their country's flag have a responsibility to screen a vessel's history prior to registering it, and to deny service if it is a UN-sanctioned vessel or has been found to be involved in sanctions-evading schemes. If found to be involved in illicit activities while registered, the vessel should be de-registered immediately and other stakeholders such as insurance companies should be alerted. If provided with intelligence or other information that warrants boarding and investigation, the vessel's registry state should cooperate with foreign governments. Once a vessel is de-registered, it forces the ship to interrupt its voyage and find a new open registry, or to use its own country's registry. In cases of Iranian or North Korean-owned ships, owners will try to avoid the latter, since an Iranian or North Korean flag would draw additional scrutiny and attention by foreign maritime or customs officers and other authorities.

Insurers and insurance brokers, or those that provide insurance and re-insurance to aircraft, ships, tankers, and their cargo, enable the movement of goods across the globe. Without a range of insurance protection, such as hull and indemnity insurance, owners will often not take the risk of operating their ship or aircraft. Even if owners are willing to take the risk, the registry, operator, manager, crew, and even the lender can intervene. These and other stakeholders need to be aware if the vessel they are covering has or is conducting illicit activity. A Treasury Department sanctions advisory recommends maritime shipment stakeholders pay attention to red flags, screen vessels' AIS histories, and potentially investigate suspicious "signs of AIS transponder manipulation."[20] It further recommends maritime insurance companies introduce a clause in their insurance contracts stating that turning off the AIS will result in an investigation and potentially a loss of coverage. Maritime intelligence services and tracking software databases, such as PurpleTRAC by Pole Star, can assist insurance companies and other stakeholders in undertaking due diligence. PurpleTRAC, for example, monitors a vessel's movement history, presence on sanctions lists, and abuse of port controls.[21]

Some insurance providers include a blanket clause in their policies that the policy becomes void when sanctions violations occur, and often refers to not only UN, but also to U.S. and EU sanctions. The aforementioned RUSI report found that companies with a close relationship to a U.S. company (such as subsidiaries or daughter companies) generally avoid business with

---

[18] See: World Customs Organization, *International Convention on the Simplification and Harmonization of Customs Procedures, Text of the Revised Kyoto Convention*, April 17, 2008, http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/conventions/pf_revised_kyoto_conv/kyoto_new/spand.aspx

[19] David Albright, Sarah Burkhard, and Andrea Stricker, *Peddling Peril Index for 2019/2020: Ranking National Strategic Export Control Systems* (Washington, D.C.: Institute for Science and International Security, 2019), http://isis-online.org/uploads/isis-reports/documents/The_Peddling_Peril_Index_Final_May2019.pdf

[20] "Updated Guidance on Addressing North Korea's Illicit Shipping Practices."

[21] See: "Purple Track," Pole Star, accessed September 11, 2019, https://www.polestarglobal.com/services/sanctions/

embargoed countries such as North Korea and Syria, but there is a general over-reliance on identifying obvious links and using basic screening lists. The report reiterates the need for insurers around the globe to conduct more comprehensive due diligence, and finds that insurance companies, while often depending on receiving accurate information from their customers or brokers, are in a unique position to share relevant illicit trade information with other insurance providers and with banks.[22]

The leverage and impact an insurance provider can have is shown in a recent example of Iranian evasion of U.S. sanctions. P&I Club, the maritime insurance provider of two vessels allegedly involved in illegal transport of petroleum, not only terminated the vessels' coverage, but it also notified the financial backer of the ships, a German-based bank. The bank initiated a court process to seize the ships, accusing the China-based owner of failing to repay a loan. The ships were temporarily detained in Singapore, but have since been released.[23] Without further information, it is difficult to assess why the ships were released, but the involvement of the ships in sanctions-busting efforts at least temporarily disrupted their efforts and raised the public profile of their actions.

[22] See: Dall and Keatinge, "Underwriting Proliferation – Sanctions Evasion, Proliferation Finance and the Insurance Industry."

[23] Saket Sundria , Serene Cheong , and Dan Murtaugh, "Iran Sanctions Breach Suspicion Prompts Bank to Seize Ships," *Bloomberg,* August 5, 2019, https://www.bloomberg.com/news/articles/2019-08-05/suspicions-of-iran-sanctions-breach-spark-china-tanker-seizures

Section IV. Special Cases

Chapter 11. MKS Pressure Transducers

In February 2014, while in Britain to attend a national soccer match, the Chinese national Sihai Cheng, also known as Alex Cheng, was arrested by British authorities pursuant to a U.S. arrest request. Two months later, on April 4, 2014, the United States District Court in the District of Massachusetts unsealed a ten count indictment against Cheng for operating as a middleman and procuring over 1,000 MKS Instruments pressure transducers from the MKS subsidiary in Shanghai, on behalf of the Islamic Republic of Iran's nuclear program.[1] The indictment focused its charges on the period 2009 to 2012, when Cheng used his trading companies Sohi Technology Co. Ltd (later renamed Vaxon Technology), and its locations in Shanghai and Hong Kong, to commit his crimes.

The arrest of Cheng marked the second arrest of a Chinese national involved in illicitly selling MKS pressure transducers in Shanghai, China.[2] Qiang Hu, a senior Chinese sales manager at MKS Shanghai, was arrested on May 17, 2012 near the Andover, Massachusetts headquarters of MKS. Hu was formally charged the next day with one count of conspiracy for violating U.S. export controls by allegedly selling thousands of pressure transducers to unnamed customers without required U.S. authorization. He pled guilty on October 16, 2013 and was subsequently sentenced on July 24, 2014 to 34 months in prison. He schemed during 2007 to 2012 to facilitate the purchase of thousands of pressure transducers by Iran and other countries (see sidebar). Hu's insider scheme, which he conducted with several other associates at MKS Shanghai, enabled, among others, Cheng's illicit procurements of pressure transducers. Hu's arrest marked a turning point in what may have been one of the more damaging insider nuclear proliferation cases in recent times.

Efforts to deceive MKS and other pressure transducer suppliers are not new, and illicit schemes involving MKS or other pressure transducers have a long history.[3] MKS pressure transducers have featured in other prosecutions or known procurements by sanctioned nuclear programs, such as by Pakistan using the A.Q. Khan network. The fact that there are only a few pressure transducer manufacturers around the globe should lend itself to more effective export controls against illegal sales of pressure transducers, which is perhaps what makes this case so egregious. However, the reality is that the insider trading scheme organized by Hu and his

---

[1] United States District Court in the District of Massachusetts, Grand Jury Indictment: United States of America v. Sihai Cheng et al., Crim. No. 13cr10332, Filed November 21, 2013. See also, Ian J. Stewart, Andrea Stricker, and David Albright, "Chinese Citizen's Involvement in the Supply of MKS Pressure Transducers to Iran: Preventing a Reoccurrence," *Institute for Science and International Security and Project Alpha, King's College London,* April 30, 2014, https://isis-online.org/uploads/isis-reports/documents/MKS_China_30Apr2014-final.pdf

[2] David Albright and Andrea Stricker, "Case Study- Chinese Salesman Arrested in Pressure Transducer Case" *Institute for Science and International Security*, January 18, 2013, http://isis-online.org/uploads/isis-reports/documents/Hu_illicit_trade_case_18Jan2013.pdf

[3] See Box 4 on previous attempts on pages 69-70 in Albright, Stricker, and Houston Wood, *Future World of Illicit Nuclear Trade: Mitigating the Threat* (Washington, D.C.: Institute for Science and International Security, July 29, 2013). Available online at: http://isis-online.org/uploads/isis-reports/documents/Full_Report_DTRA-PASCC_29July2013-FINAL.pdf

colleagues was, by its very nature, difficult to detect. It is to the credit of U.S. enforcement that it was able to detect it and prosecute at least two key members involved in the scheme, including a ringleader and a principal customer. Looking back, one of the few indications for U.S. export authorities that a scheme existed was the unusual uptick in the number of pressure transducers sent to MKS Shanghai from the headquarters, but that uptick also could signal increased success in selling a product.

The Cheng case provides unique insights into the operation of Iran's illicit procurement efforts and the techniques and motivations of Chinese agents, who remain major facilitators of proliferation. The basis of this chapter is drawn from public evidence from the Cheng case. The evidence was gathered by the U.S. Attorney's Office for the District of Massachusetts, in cooperation with the Boston offices of the Federal Bureau of Investigation (FBI), U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), and the Commerce Department's Office of Export Enforcement (OEE). The evidence contains tens of thousands of e-mails and Microsoft MSN Chats obtained by search warrants or recovered by the FBI from Cheng's computer when he was arrested in Britain. The MSN Chat record involves texts between Cheng and his main co-conspirator, Iranian national Seyed Abolfazi Shahab Jamili, and includes over 60,000 lines of chat from early 2006 into 2013 and innumerable details about orders, payments, successes in acquiring sensitive goods, and many travails in filling orders for pressure transducers. Their efforts also involved procuring additional goods for Iran's gas centrifuge program, other nuclear programs, and conventional military programs, as well as obtaining non-sensitive goods for automobile manufacturing and other civilian uses. Typical of chats, the texts are filled with misspellings, shortenings, and symbols. When quoting chats and e-mails, no effort has been made to edit the text or highlight errors, unless needed for clarity.

A chapter in Volume 2 of this report that is confidential discusses additional evidence in the Cheng case. It delves more deeply into Cheng and Jamili's activities on behalf of Iran.

Background on Cheng's Indictment and his Co-Conspirators

The original secret, or sealed, U.S. indictment was returned on November 21, 2013, charging Cheng and Jamili -- as well as two corporate defendants -- Nicaro Eng. Co., Ltd, and Eyvaz Technic Company -- with conspiracy, smuggling, and unlawful export to Iran of highly sensitive United States-manufactured goods with nuclear applications, in violation of U.S. laws and regulations. Cheng worked with Jamili from about 2005 to 2013 to supply Iran with nuclear dual-use goods and materials for "Iranian government work" using Jamili's company, Nicaro Engineering in Tehran. Nicaro in turn often contracted with Eyvaz Technic, also located in Tehran, which received contracts from the Iranian centrifuge program for the supply of a range of goods. In addition to procuring goods itself internationally, Eyvaz made products for the centrifuge program in its factory in Tehran, while Nicaro was strictly a trading company.

Eyvaz Technic Company was established in 1993 and was involved in both obtaining goods from abroad and making a line of equipment for the oil and gas industry. Its work for Iran's gas

centrifuge program was secret and led the European Union in 2011 to designate Eyvaz for supplying vacuum equipment to Iran's enrichment facilities. The Cheng indictment states that the EU "found that Eyvaz had produced vacuum equipment, which it supplied to two of Iran's uranium nuclear enrichment facilities, Natanz and Fordow."[4]

On December 18, 2015, Cheng pled guilty to the first six counts of the indictment, pursuant to a plea agreement with the government. The counts included conspiracy to commit export violations and smuggle goods from the United States, and export of U.S. goods, namely pressure transducers, which are used, among other applications, to develop weapon-grade uranium in gas centrifuges. Cheng exported these to Iran without first obtaining the required licenses and authorizations from the U.S. Department of Treasury. Four other counts were dismissed. On January 27, 2016, following a hearing, Federal Judge Patti Saris sentenced Cheng to nine years' imprisonment. She did not impose any term of supervised release, since Cheng is not a U.S. citizen and will be deported to the People's Republic of China (PRC) after he completes his term of imprisonment.

Neither Jamili nor any employees at Eyvaz, including its founder and head Ghaffar Shabani, have been arrested or prosecuted by the United States. The U.S. government attempted to have Jamili extradited from Iran, which included requesting that Interpol issue a red-notice for his arrest.[5] Iran refused to extradite Jamili. However, according to the Cheng sentencing memorandum, "On January 16, 2016, the U.S. Attorney's Office was directed by Washington to dismiss the charges against Jamili as part of the agreement between the United States and the Government of Iran to release unlawfully imprisoned U.S. citizens being held in Iran."[6]

MKS Pressure Transducers

MKS Instruments, with distributors throughout the world, is a key manufacturer of capacitance manometer-based pressure transducers. This instrument, which is dual-use in nature, can be used in centrifuge plants to accurately measure operating pressure.[7] Large numbers of pressure transducers are typically used in a centrifuge plant to monitor and control the vacuum in the centrifuges and the metal piping connecting the centrifuges into cascades, and more generally, in piping running throughout the centrifuge plant. Centrifuges, which spin rapidly, operate under vacuum primarily to keep the high-speed rotor of the centrifuge from

[4] *Grand Jury Indictment: United States of America v. Sihai Cheng et al.*

[5] *Government Sentencing Memorandum*, *U.S. District Court, District of Massachusetts, USA vs Sihai Cheng,* Crim. No. 13-10332-PBS, Document 83, Filed January 22, 2016, p. 7.

[6] Ibid.

[7] Cheng and Jamili often referred to the pressure transducers as pressure transmitters, which are variations of the same equipment. In fact, the difference between the two is slight. The main difference is the kind of electrical signal each sends, where a transducer sends a signal in volts and a transmitter sends a signal in milliamps. For situations where the electrical connections are short, a pressure transducer is better. They are also often smaller and have fewer electronic components that can be disrupted by electromagnetic interference. See: https://www.esi-tec.com/blog-pressure-sensors-transmitter-transducer/2012/01/what-is-the-difference-between-a-pressure-transducer-and-transmitter

overheating due to friction. Moreover, a centrifuge plant operates with a highly corrosive gas, uranium hexafluoride. MKS pressure transducers, beyond being highly accurate at extremely low pressures, are made of corrosion-resistant materials, such as Inconel. Thus, pressure transducers are key to the successful operation of a centrifuge plant, and MKS manufactures some of the best ones in the world.

Because they are very difficult to make, pressure transducers have been a key item that Iran, North Korea, and Pakistan, among others, have had to acquire overseas to build and operate covert gas centrifuge plants. Moreover, these pressure transducers have a limited lifespan. Therefore, a consistent supply has been necessary for Iran and other enrichment programs to continue to operate centrifuge plants. This dependence and resulting vulnerability have motivated Iran to seek the domestic capability to build pressure transducers (see Chapters 4 and C.2). However, this effort has depended on Iran acquiring key subcomponents from abroad.

Vacuum pressures inside gas centrifuge cascades, and thus the types of pressure transducers needed, are well defined. Inquiries by would-be customers about certain pressure transducers in relatively large quantities typically increase suspicion of intended centrifuge use. The pressure transducers ordered by Cheng match the expected ones for a centrifuge plant.

The use of MKS pressure transducers in Iranian centrifuge plants is demonstrated in well-publicized 2008 images of the former president of Iran, Mahmoud Ahmadinejad, touring Iran's Pilot Fuel Enrichment Plant (PFEP) at Natanz. The photographs show that a single, advanced test centrifuge has one MKS pressure transducer and a pilot centrifuge cascade has many of them (see Figures 11.1 and 11.2).

Figure 11.1. Iranian president Mahmoud Ahmadinejad examines an advanced gas centrifuge test stand at the Natanz pilot fuel enrichment plant during a 2008 visit. An MKS pressure transducer can be seen. The MKS pressure transducer in the image appears to be a series 600, perhaps a 622 or 626 model. Cheng and Jamili sought newer models, namely 722A and 722B series during 2009-2011, which are smaller and more economical. Image source: Website archive of the president of Iran, www.President.ir.

Figure 11.2. President Ahmadinejad examines gas centrifuge equipment, which includes an MKS pressure transducer (next to his right hand) during a visit to the Natanz pilot fuel enrichment plant in 2008. In the background is an IR-1 gas centrifuge cascade which contains many more recent (mid-2000s) models of MKS pressure transducers. Image source: Website archive of the president of Iran, www.President.ir

Insider Scheme at MKS Shanghai

Cheng and Jamili's secret purchase of MKS pressure transducers in China depended on a multi-year insider scheme from 2007 to 2012, centered at MKS Shanghai, to illegally export MKS pressure transducers and apparently other sensitive MKS products from the United States.[8] The leader of this scheme was Qiang Hu, aka Johnson Hu, a Chinese citizen, who was the sales manager at this subsidiary of MKS, where the headquarters is based in Andover, Massachusetts. He was hired in 2008 by his brother-in-law, Steven Yao, who was the general manager and is believed to be the person who originally developed the illegal exporting scheme at MKS Shanghai.

In addition to Yao, Hu conspired with five other Chinese nationals. Xiao Lu ("Lu") was a salesman who worked for Hu at MKS Shanghai. Candy Meng was the subsidiary's logistics and purchasing manager. Sara Zhou worked there in logistics, and Lily Lee worked in purchasing and accounting. Wang Ping was an independent middleman who used at least two front companies to help Hu and Lu obtain and complete illegal export transactions.

Wang Ping's principal company was based in Shanghai and was called Racy System Integration Co. Ltd. His second company was a Hong Kong-based entity, Wang Chao International Trade Co. Ltd.

Hu and his associates used two primary methods to deceive MKS headquarters, obtain U.S. export licenses, and deliver pressure transducers and other sensitive parts to illegitimate end-users in China.[9] All the parts were made at MKS in Andover and shipped to MKS Shanghai for purported sale to legitimate customers, with a U.S. export license. To deceive the Andover headquarters, Hu and Lu used the export licenses of other, legitimate MKS customers to acquire the goods, and then delivered the goods to Wang Ping. He in turn supplied them to the actual purchasers, who were not listed on the export license. Because most customers require multiple pressure transducers, MKS Andover would apply for a license to export and sell a fixed quantity of goods to an end-user over a set period, typically two years. That quantity could vary, but could reach 200 or more pressure transducers. Hu and Lu exploited this procedure to obtain extra pressure transducers that could be sold to other end-users illegally. These extra pressure transducers would be falsely listed on intra-company purchase orders as being sold to the previous, legitimate end-user.

Hu and Lu also used another method to deceive MKS Andover, whereby they declared false end-users to MKS Andover, in particular using Racy System. MKS Andover would then apply

[8] U.S. District Court in the District of Massachusetts, *Government Sentencing Memorandum, United States versus Qiang Hu,* Case 1:12-cr-10188-PBS, Document 84, Filed July 18, 2014. This sidebar draws heavily on this memorandum.

[9] For more details on the case and the methods used, see Albright and Stricker, "Case Study- Chinese Salesman Arrested in Pressure Transducer Case."

for a U.S. export license for this false end-user. In the case of Racy System, the conspirators stated that the parts would be used to manufacture medical plasma cleaning systems.

This scheme required MKS Shanghai to maintain two sets of books. One set, the accurate one, was shared only among the conspirators and showed the company or person that actually purchased the goods. This set contained the export license, the price paid by the customer, and the delivery addresses to use after MKS Shanghai received the goods from Andover. The other set of books, which were phony, were shown to representatives of MKS Andover when they performed audits. These records showed all the goods going to only authorized end-users.

Hu and his co-conspirators, on average, charged a 40 percent markup on their illegal sales from 2007 to 2012, which in total, included thousands of MKS pressure transducers. In Hu's plea, he agreed to a set of facts, including, "As a result of this conspiracy and the illegal activities of Hu and his conspirators, thousands of export-controlled MKS pressure transducers, worth millions of dollars, were exported from the US and delivered to unknown and unauthorized end-users in the PRC and elsewhere."[10] A full list of these purchasers, beyond Cheng's purchases from 2009 to 2011 and unidentified Chinese entities, has not been revealed. As the quote states, determining the ultimate, and possibly current users, of the thousands of pressure transducers may be impossible without more assistance from the co-conspirators. One can speculate that the non-Chinese end-users may have included North Korea's and Pakistan's centrifuge programs. In addition, Iran's centrifuge program may have benefited from working with MKS Shanghai agents prior to 2009.

Significance of Procurements

According to the U.S. investigation, Cheng and Jamili succeeded in supplying 1,185 MKS pressure transducers to Iran's gas centrifuge program from 2009 into 2011.[11] How many does Iran's centrifuge program need? Was their supply significant?

The Institute has estimated, based on the large number of pressure transducers that are visible in the cascade at the PFEP, as seen in Figure 11.2, that Iran likely uses about one pressure transducer per ten centrifuges in the cascade at the PFEP. This density equates to about 16 pressure transducers per cascade, which corresponds to roughly one pressure transducer per enrichment stage in Iran's IR-1 centrifuge cascade, which have typically had 15-17 enrichment stages. However, it may be that fewer pressure transducers are needed in a production cascade in the Fuel Enrichment Plant (FEP) at Natanz and at the Fordow Fuel Enrichment Plant (FFEP). The number in the cascade itself is supplemented by other pressure transducers used in the piping that transfers uranium hexafluoride feed gas into the cascade and enriched uranium product and depleted uranium waste out of the cascade after passing through the centrifuges.

[10] *Government Sentencing Memorandum, United States versus Qiang Hu.*

[11] *Government Sentencing Memorandum, USA vs Sihai Cheng*.

Iran's centrifuge designs, both individually and collectively in cascades, are based on Pakistan's centrifuges. From Pakistani cascade drawings obtained in the prosecution of Khan network members in Switzerland, it is evident that one pressure gauge was used per stage in a cascade, and a handful were used in the rest of the cascade. The diagrams indicated that one Pirani gauge, which derives a pressure reading from thermal conductivity, was used in each stage of the cascade, but pressure transducers could also be used and would be more accurate in the pressure regions encountered in the stages of a centrifuge cascade. Thus, Iran may indeed use many pressure transducers in each cascade.

At Iran's two production-scale enrichment plants at Natanz and Fordow, at the time of Cheng and Jamili's purchases, the centrifuge cascades were organized into modules, each containing 18 IR-1 production cascades that contain, in total, about 3,000 IR-1 centrifuges and large amounts of piping associated with feeding and withdrawing uranium from the centrifuges. Although the exact number of pressure transducers used in an Iranian centrifuge cascade is not available publicly, as reasoned above, if one pressure transducer is used for each enrichment stage, and 15 stages are assumed, with five more pressure transducers used in other parts of the cascade system, including what is called the dump system, then there is an estimated total of 20 pressure transducers in each cascade. Any pressure transducers used outside the cascade areas, but within the piping of the module, are ignored here. Then, 18 production cascades would require 360 pressure transducers. By early 2012, Iran had installed a total of 58 IR-1 cascades in four modules in these two plants,[12] and with the estimate above, would have required 1,160 pressure transducers. About a year later, in early 2013, Iran had installed a total of 89 IR-1 cascades in five modules,[13] requiring, in total, an estimated 1,780 pressure transducers, ignoring spares and breakage. In any case, the overall number of pressure transducers needed for the FEP and Fordow plants was thus very large and Cheng and Jamili's procurement of 1,185 pressure transducers was quite significant in meeting the total requirements for pressure transducers up to 2012/2013. If fewer pressure transducers were used per cascade, then their contribution would have been even more significant.

Supporting this finding are statements by the end-user, the Iranian centrifuge program's procurement office, and Eyvaz, expressing great value for Cheng and Jamili. For example, Eyvaz considered Cheng an important supplier. Jamili told Cheng on June 3, 2011, "Their warehouse [end user] quantity is enought for their next 6 months projects."[14] He added that the

[12] See: Albright, Paul Brannan, and Christina Walrond, "ISIS Analysis of IAEA Iran Safeguards Report," *Institute for Science and International Security,* February 24, 2012, http://isis-online.org/uploads/isis-reports/documents/ISIS_Analysis_IAEA_Rerport_24Feb2012.pdf The fourth module would have had only four cascades installed as of that date.

[13] See: Albright, Walrond, Stricker, and Robert Avagyan, "ISIS Analysis of IAEA Iran Safeguards Report," *Institute for Science and International Security,* February 21, 2013, http://isis-online.org/uploads/isis-reports/documents/ISIS_Analysis_IAEA_safeguards_Report_21Feb2013.pdf

[14] MSN Chat, Government Exhibit 24.

centrifuge procurement office had "not teceived new purchasing project from their top management. Of course, if they will receive new order, we are their number 1 sorce."[15]

The Scheme

Cheng and Jamili had been working together since 2005, supplying goods to Iran's nuclear and military programs (see Volume 2, Chapters C.1-C.3). They had navigated several successful procurements and had become comfortable as a team. They felt competent to compete in the complex world of Iranian illicit procurements. Iranian trading companies competed intensely for the contracts of the centrifuge and other proliferation programs, where undercutting, betraying, and double dealing by one another was common. Given that most of the procurements were illegal and sanctions on Iran were tightening, leading more suppliers to avoid business with Iran, failure was an ever-present aspect of business, including the risk to have funds and goods seized abroad. Succeeding in the face of these growing hardships became an increasingly important factor in winning bids from the nuclear programs.

For many of the pressure transducer procurements, the actual end-user, i.e. the centrifuge program, contracted with Eyvaz, which in turn offered Nicaro the tender to acquire the goods. Eyvaz had established direct contact with the procurement office of the centrifuge program and was trusted by it, according to Jamili. Jamili and Cheng avoided naming the end-user in their correspondence but occasionally referred to it as Kalaye Electric. Up until at least 2013, Kalaye Electric was the name of a major site of Iran's centrifuge research and development in Tehran and also the name of the company building the centrifuge plants. It also procured critical goods for Iran's centrifuge cascades.[16] Kalaye Electric was sanctioned by the United Nations Security Council in 2006 under Resolution 1737 for carrying out undeclared uranium enrichment research and development. The United States also designated Kalaye Electric as a proliferator of WMD in 2007.

However, this additional layer in the supply chain occupied by Eyvaz caused friction with Cheng and Jamili over the pace of inquiries and payments. The centrifuge program would pay Eyvaz, which in turn would pay Jamili, who would transfer the funds out of the country to Cheng, typically through an intermediary country. It also meant that Eyvaz could approach more than one trading company to get goods, further adding to tensions. Jamili, not surprisingly, tried to establish direct contacts with the centrifuge program procurement office to better his chances of winning bids.

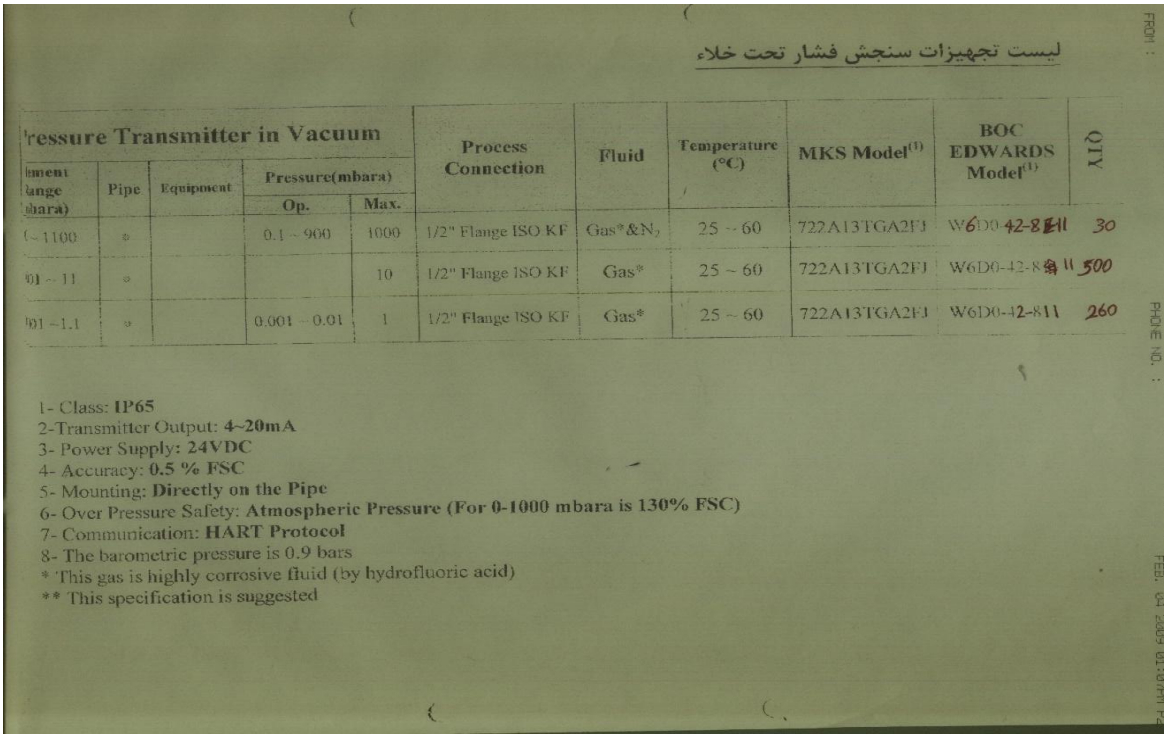
First Inquiry

Jamili and Cheng were excited about receiving their first inquiry for pressure transmitters from Eyvaz. In an e-mail in February 2009, Eyvaz asked Jamili if he could procure 790 pressure

[15] Ibid.

[16] Wisconsin Project on Nuclear Arms Control, "Kalaye Electric Company," Updated May 15, 2015, https://www.iranwatch.org/iranian-entities/kalaye-electric-company

transmitters and attached a copy of Eyvaz' inquiry (see Figure 3).[17] Jamili told Cheng in the e-mail that Eyvaz could no longer buy them directly in England due to a new limitation. However, Eyvaz informed Jamili that the British vacuum firm, Edwards, had an agent in China who might be able to supply them after direct purchase from Britain was no longer possible.



لیست تجهیزات سنجش فشار تحت خلاء

'ressure Transmitter in Vacuum

ument ange bara)	Pipe	Equipment	Pressure(mbara) Op.	Max.	Process Connection	Fluid	Temperature (°C)	MKS Model(1)	BOC EDWARDS Model(1)	QTY
~1100	*		0.1 ~ 900	1000	1/2" Flange ISO KF	Gas*&N_2	25 ~ 60	722A13TGA2FJ	W6D0-42-8[illegible]	30
01 ~ 11	*			10	1/2" Flange ISO KF	Gas*	25 ~ 60	722A13TGA2FJ	W6D0-42-8[illegible]	500
001 ~1.1	*		0.001 ~ 0.01	1	1/2" Flange ISO KF	Gas*	25 ~ 60	722A13TGA2FJ	W6D0-42-811	260

1- Class: **IP65**
2-Transmitter Output: **4~20mA**
3- Power Supply: **24VDC**
4- Accuracy: **0.5 % FSC**
5- Mounting: **Directly on the Pipe**
6- Over Pressure Safety: **Atmospheric Pressure (For 0-1000 mbara is 130% FSC)**
7- Communication: **HART Protocol**
8- The barometric pressure is 0.9 bars
* This gas is highly corrosive fluid (by hydrofluoric acid)
** This specification is suggested

Figure 11.3. Inquiry from Iranian centrifuge program, via Eyvaz, for an order of 790 pressure transmitters. The Farsi in the top right corner is "Vacuum Pressure Measurement Equipment List." The fax has a date of February 4, 2009 but the sender is blank.

The inquiry from Eyvaz listed the specifications and numbers needed and provided their model numbers for both MKS and BOC Edwards (now called Edwards) (see Figure 11.3). That the model numbers are the same in each row is contradictory with the difference in specifications. The MKS model sought was a 722A series, which were advertised as smaller and more economical. Based on the specifications on pressure in the inquiry, the numbers and actual MKS model numbers requested are listed in Table 11.1 at the end of this chapter.[18]

The inquiry asked only for the pressure transducer with model number 722A13TGAFJ, and this mistake was never explained. Later in the process, the MKS Shanghai agent clarified this mistake to Cheng and Jamili and provided the correct model for the different pressure regimes of interest in the inquiry.[19]

[17] *Government's Sentencing Memorandum, USA vs Sihai Cheng*.

[18] Ibid.

[19] The pressure regime given was for one with a full-scale reading of 1000 torr; the model numbers for full-scale reading of 10 and 1 torr are 722A11TGAFJ and 722A01TGAFJ, respectively.

Table 11.1 List of Full-Scale Pressure and Type of MKS Pressure Transducers Sought

Maximum Pressure on Scale* Desired	Corresponding 722A series[20]	Number
1000 mbar	722A13TGAFJ	30
10 mbar	722A11TGAFJ	500
1 mbar	722A01TGAFJ	260
	Total	790

*Pressure in the inquiry is measured in millibar, a standard unit in Britain. MKS uses the unit of torr, where 1 millibar (mbar) equals 0.75 torr. Thus, for MKS pressure transducers, the full-scale reading is usually stated in torr, or for the models of interest to Iran, as having a maximum pressure, or a full-scale reading, of 1, 10, or 1000 torr.

The inquiry did not explicitly state the gas was uranium hexafluoride, but it implied it. For example, the inquiry specified that the intended gas would be highly corrosive and involve corrosion products such as hydrofluoric acid. Uranium hexafluoride, when exposed to water, such as water vapor in the air, breaks down into hydrofluoric acid.

The range of pressures measured are consistent with a centrifuge plant. However, the need for so many pressure transducers with a full-scale reading of 1 mbar is difficult to understand. Typical pressures in the centrifuges and associated piping are usually at least several millibar (mbar), or equivalently in the units preferred by MKS, several torr. Of the total number of pressure transducers ultimately supplied to Eyvaz, over 95 percent of the pressure transducers had a full-scale reading of ten torr, where one mbar is about 0.75 torr.[21]

After receiving Jamili's inquiry, Cheng contacted MKS Shanghai. It is unknown if he also contacted Edwards' agent in China. Cheng managed to contact MKS's agent Wang Ping (referred to in the Cheng indictment as Co-conspirator #1), who was involved in the insider scheme led by Hu at MKS Shanghai (see previous Sidebar). According to the Sentencing Memorandum:[22]

> With the knowledge and agreement of several employees at MKS-Shanghai, Wang Ping set up two front companies in China, Racy System Integration Co., Ltd. and Wang Chao International Trade Co., Ltd., to pose as the end-user in transactions with the MKS-Shanghai for the purpose of fraudulently obtaining export licenses from the United States. These two companies were owned and operated by Wang Ping.

[20] These MKS model numbers refer to the full scale reading in torr, where one torr equals 1.33 mbar.

[21] Government Exhibits 3 and 14, and Table 11.2.

[22] *Government's Sentencing Memorandum, USA vs Sihai Cheng.*

In a May 14, 2009 e-mail to Jamili, Cheng described how he arranged the first orders:[23]

> When I contact MKS Shanghai office, they tell me I should contact their Shanghai agent since I am in Shanghai. I told them my customer is in Singapore, they said OK if it's sold not in China. They asked many questions about my *Singapore customer*'s information. I insisted that's commercial secret and did not tell them. So they refused to negotiate business with us, and they refused to tell me their Shanghai agent's information. I had no way but ask another friend in Ningbo electronics factory to contact them and got Shanghai agent's information. Then I called this agent and I proposed to meet face to face.
>
> This agent also cared much about who is the real end user. He clearly told me that he hope this Singapore customer should be the real end user, and could not be supplied to the Middle East! I promised to him that it's really supplied to Singapore. He asked whether it's possible that this Singapore customer would resell to others, I said I don't know. He hesitated to take this risk, since if it's revealed finally these goods enter the Middle East, he will lose the agency for ever and will be punished by MKS. I have to allure him with the big quantity. He hesitated and said he cannot made the decision. I asked him what he was afraid of, he expressed his worry: each product with a series no, and with these numbers MKS know which agent these products are from, and he worried that the payment record between his company and my company will be another proof in the future. I told him whether the series no. is crucial for application, he said no, then I proposed I will contact customer to ask whether it's OK to erase the series no., he agrees. As for the payment channel, I propose I sign the contract with his company but in the contract we regulate the money should be paid to another company's bank account (it's his relative's company), but all the duty and responsibility lie only between my company and his own company. Finally he agrees, and he proposed the last condition, that is, I cannot ship the products from Shanghai ! I will have to ship the goods from Hong Kong. With such complicated arrangement, he agreed that it's hard to trace these products!

In this e-mail, Cheng added for emphasis: "WE ONLY HAD VERY GOOD LUCK TO MEET A PERSON WHO LOVES MONEY TOO MUCH!." Given the long term, corrupt nature of the staff at MKS Shanghai, the agents were not difficult to convince to sell pressure transducers to their new customer.

MKS headquarters was kept in the dark. Cheng told Jamili in 2009, referring to pressure transducers, "the goods are supplied to us SECRETLY! MKS doesn't know it's [sic] supplied to me!"[24] He added that MKS was being deceived about the end-user. "They think it's supplied to

[23] E-mail from Alex Cheng to Nicaro Engineering, Jamili, Subject: pressure transmitter, May 14, 2009. From Government Exhibit 10.

[24] E-mail from Alex Cheng to Nicaro Engineering, Jamili, Subject: pressure transmitter, May 14, 2009.

the Shanghai agent and used for some Chinese solar energy and semiconductor industry, never expecting that this supplier dare to supply me."[25]

According to MKS procedures, the original inquiry for 790 pressure transmitters should have been sent to MKS headquarters in Massachusetts but was instead handled in Shanghai. The group in Shanghai shared its phony order and accounting books with the U.S. headquarters and kept the one that was accurate to themselves (see previous Sidebar).

Pressure transducers are relatively expensive, and price was an issue for Eyvaz. The end-user was unwilling to accept the initial price given by MKS Shanghai, and Cheng had to negotiate a lower price per item. According to Cheng:[26]

> As for the price, I really did a looooooooooooooooooooot of work to persuade them to give the discounts twice. Your end user must be very satisfied with everything. You know I have profit only 2%. (The supplier tells me he has 5% profit).[27]

The price set at the end of these negotiations in February 2009 was $1,850 per pressure transducer. The Iranian side still thought the price was too high, and Cheng negotiated a slightly reduced price of somewhat less than $1,800 per pressure transducer, which involved Cheng taking a smaller commission.

For legitimate customers, the price of the pressure transducer Cheng sought was considerably less. They were much closer to $1,000-1,200 apiece at the time of these purchases. This means that Hu and his colleagues, including Wang, were marking up the price considerably for the less savory customers (see Chapter C.4 for further discussion of the prices). In addition, Cheng and Jamili added their fees.

The payment terms were 30 percent as a deposit and 70 percent before shipment. Cheng received the payments as an international wire of funds, or as a telegraphic transfer (T/T). Subsequently, the prices declined slightly but not by very much.

According to the Sentencing Memorandum:[28]

> Between 2009 and 2011, Cheng placed orders with Wang Ping for more than 1,000 MKS pressure transducers. As a result of Cheng's orders, MKS pressure transducers were shipped from Andover, Massachusetts to Shanghai, China. Once the parts were shipped to Shanghai, Cheng inspected them and removed the serial numbers and then shipped the parts to Hong Kong and from Hong Kong, Cheng exported them via DHL or another

[25] Ibid.

[26] E-mail from Alex Cheng to Nicaro Engineering, Jamili, Subject: pressure transmitter, May 14, 2009.

[27] Ibid.

[28] *Government's Sentencing Memorandum, USA vs Sihai Cheng*, p. 16.

courier service to Eyvaz or Jamili in Tehran, Iran. For these exports, Eyvaz and Jamili paid Cheng over 1.8 million dollars.

The initial orders were for series 722A pressure transducers, but in 2010, this model became obsolete. Subsequently, Cheng ordered the equivalent 722B series of pressure transducers. Figure 11.4 shows a 722 series pressure transducer.

Figure 11.4. Image of a 722 series pressure transducer from MKS' web site, similar to those ordered by Cheng for Iran. This one has a full-scale reading of one torr.
https://www.mksinst.com/f/722bcompact-absolute-capacitance-manometers

Typically, the MKS Shanghai agent imported the pressure transducers from the United States to Shanghai. As agreed with the MKS agent and communicated to Jamili, after inspecting them, Cheng removed their serial numbers, concealing their shipment to China (see Figure 11.5). This way, if seized during shipment, they could not be traced back to MKS Shanghai.

After initially accepting the removal of the serial numbers, the Iranian centrifuge procurement office later expressed worry about whether the pressure transducers were 100 percent made in the United States or used parts from elsewhere. In other cases, the Iranian centrifuge program worried about not receiving goods from high-quality Western suppliers.

For example, in one case in April 2011, Jamili advised Cheng that the end-user had expressed concern that the pressure transducers from Cheng were in fact not manufactured in the United States because the serial numbers and labels had been removed.[29] In an April 11, 2011 chat,

[29] *Government's Sentencing Memorandum, USA vs Sihai Cheng*, p. 18.

Cheng confirmed that the pressure transducers he was exporting to Iran were all manufactured in the United States:

> Jamili: are you sure they are supplying to you from USA factory?
> Cheng: what do you mean?
> Cheng: yes, it's from USA
> Cheng: I saw everything on the carton
> Cheng: it's shipped from the usa to shanghai
> ***
> Cheng: every time I remove the label from the carton!
> Cheng: becasue [sic] I worry it causes big risk!

To assure his buyers, Cheng had been sending Jamili photographs of the pressure transducers in their original packing cartons and with their serial numbers removed (see Figure 11.5). Figure 11.6 shows the original shipping cartons received from MKS Andover and sent to MKS Shanghai.

Figure 11.5. An MKS pressure transducer with serial number removed by Cheng. It is a 722A, 10 torr full-scale pressure transducer. Compare to Figure 11.4, where the serial numbers are visible on a similar pressure transducer. Source of image: Government Exhibit 14.

Figure 11.6. Cheng's photo of the original shipping cartons sent from MKS headquarters in Andover, Massachusetts to Lily Lee, one of the co-conspirators at MKS Shanghai.

Unlike the previous prosecution of Hu and his diversion of MKS pressure transducers, where diversion to Iran was not categorically established, at least in public documents, the evidence in the Cheng case makes many direct links with Iran's gas centrifuge program. The mention of Kalaye Electric, as discussed above, is one such link.

Moreover, Cheng was aware that the pressure transducers were for a secret and sensitive project.[30] He even knew they were for a nuclear program and indeed for Kalaye Electric, as evidenced by MSN Chat. In chat records between Cheng and Jamili, Cheng expressed awareness that he was supplying parts to Kalaye Electric and this company was not a strictly civil one. Cheng looked up this facility on Google and the web page he found described Kalaye Electric in 2009 as a "supplier to Iran's weapons industry," and linked to WMD.[31]

At the time Cheng and Jamili were receiving their first inquiry for pressure transducers, the Fordow centrifuge plant was being built secretly and was entering a period when procurements

[30] *Government's Sentencing Memorandum, USA vs Sihai Cheng*, p. 3.

[31] Ibid, p. 4.

would be occurring for the plant's centrifuge cascades. Based on subsequent reporting by inspectors of the International Atomic Energy Agency (IAEA) in late 2009 and documents from an Iranian Nuclear Archive seized by Israel in early 2018, the Fordow enrichment site was being built in the early 2000s to make weapon-grade uranium for nuclear weapons.[32] After Iran downsized its nuclear weapons program in late 2003, it nonetheless continued the secret construction of the Fordow enrichment site to make weapon-grade uranium.[33] After its discovery and exposure by Western countries in October 2009, Iran repurposed the site to make low enriched uranium, although it could still be modified relatively easily to make weapon-grade uranium. Thus, Cheng and Jamili were likely procuring pressure transducers for the Fordow plant and contributing directly to Iran's nuclear weapons activities. Although Cheng would not have been privy to classified information about Fordow's existence in early 2009, when he later became aware of possibly contributing to Iran's nuclear weapons program, he did not seem to care. This is part of the reason for his long prison sentence.

Means of Deception

The order for the pressure transducers was divided into numerous batches on the advice of the Iranians in order to reduce the likelihood that MKS headquarters would realize that the goods were being diverted. The Iranian procurement office decided that large orders of pressure transducers would also risk attracting too much attention from the United States and its allies. As a result, even though the initial inquiry concerned 790 pressure transducers, Jamili was told to buy in lots of about 50-150 pieces at a time. In terms of deceiving MKS headquarters, the Shanghai MKS conspirators subsequently told Cheng that they were comfortable ordering up to 200 pressure transducers from headquarters at a time.

MKS Shanghai staff, according to the indictment, knowingly used the *bona fides* of numerous Chinese companies and the Hong Kong location of Sohi Technology Co. in order to acquire or illegitimately use U.S. export licenses. MKS staff used details of two real customers of MKS Shanghai Ltd. and the two companies that were created by Wang Ping, when placing the intra-company requests to the MKS Andover office. Thinking that the declared end-users were legitimate, Andover, in turn, submitted license applications to the U.S. Commerce Department where necessary or authorized the shipment and release of goods under existing customer-specific licenses. Wang Ping served as the temporary recipient of the goods in Shanghai, in addition to Sohi Technology Co.'s location in Hong Kong, until Cheng could send them to Nicaro or Eyvaz.[34]

[32] David Albright, Frank Pabian, and Andrea Stricker, "The Fordow Enrichment Plant, aka Al Ghadir - Iran's Nuclear Archive reveals Fordow was built originally to make weapon- grade uranium for 1-2 nuclear weapons per year," *Institute for Science and International Security*, April 25, 2019, http://isis-online.org/isis-reports/detail/the-fordow-enrichment-plant-aka-al-ghadir/8

[33] Ibid.

[34] *United States of America v. Sihai Cheng et al.,* Filed November 21, 2013.

The total number of participants in this conspiracy is difficult to determine. According to the Sentencing Memorandum:[35]

> Based upon Cheng's own admissions in a chat message to Jamili, their conspiracy involved at least "6 to 7 people" in China, Iran, and the United States. On November 17, 2010, Cheng explained to Jamili in chat messages that "many people are involved" in their conspiracy. Cheng indicated that "6 to 7 parson [sic] at all [know], me, you, GS[36] [an Eyvaz officer presumably in Iran], one manager at end user side, china agent, mks manager and one person in usa."

The identity of the person in the United States is unknown, and Cheng may have been speculating in any case.

In carrying out his procurements, Cheng actively took steps to deceive MKS and customs officials, as well as other government officials, about the end use of the MKS pressure transducers. He divided the pressure transducers into smaller cartons when he was transshipping them to Iran. This tactic of using smaller boxes helped ensure that customs officials at intermediate stops would be less likely to inspect the boxes. To further reduce the risk of inspection by customs authorities, Cheng also sent the smaller boxes to different addresses in Iran, for example one to Eyvaz and another to Nicaro.

The first four orders involved each about 30-60 MKS pressure transducers, and stretched from about late April 2009 until late August 2009 (see Table 11.2). These four shipments contained in total 185 series 722A pressure transducers and were shipped in a total of seven cartons.

There was a nine-month gap between the last delivery of this first batch and first delivery of the second larger order, which involved a total of 1,000 MKS pressure transducers. The first order in this second batch was for 100 pressure transducers and it was shipped to Iran in multiple cartons in about May 2010. This order was followed by four more shipments of 100 pressure transducers each. The last two shipments, sent in the first quarter of 2011, were for 200 and 300 pressure transducers, respectively. Again, the shipments were in multiple cartons.

Since pressure transducers are relatively light in weight, Cheng's preferred method of shipment from Hong Kong to Iran was via a non-U.S. express shipper. The shipments of pressure transducers went from MKS Andover to Shanghai; from there, the MKS Shanghai officials shipped the boxes to Hong Kong, sometimes using Federal Express (see Figure 11.6). In general, they wanted to avoid using Federal Express and UPI since they are U.S. companies. In Hong Kong, Cheng repackaged them into non-descript parcels and arranged to send them to Iran via DHL.

[35] *Government's Sentencing Memorandum, USA vs Sihai Cheng*, p. 23.

[36] G. Shabani, President of Eyvaz.

Cheng and Jamili had competed with others for this 1,000-piece order and managed to win the bid (see Chapter C.4 for a further discussion of some of these difficulties). As can be seen in Table 11.2, the vast majority of the procured pressure transducers had a full-scale value of 10 torr and were likely for use in the production-scale cascades at Fordow and Natanz.

Cheng regularly complained about the difficulty of getting payments from his Iranian clients. Part of this reflected the difficulty of moving Iranian funds offshore, but another reason was the Iranian procurement office's hesitancy to pay the agreed prices. This situation was aggravated by the relatively large number of companies involved. As a result, there were many individuals taking commissions in China and Iran, driving up the price and complicating the negotiations.

Growing concerned about U.S. authorities uncovering their illegal procurements, Cheng and Jamili developed codewords for pressure transducers. Initially, in 2010, they agreed to call them "caterpillar parts." A few months later, they thought that codename was cumbersome to have to retype in chats, so after some discussion they settled on "electronic current indicator," rejecting potential terms like "controller" as sounding too sensitive. They adapted the acronym ECI to shorten it.

Quest for More Orders

Throughout 2011, Cheng was anxious to sell more to the centrifuge program. He and Jamili had originally expected to sell 3,000 pressure transducers. According to the MSN Chat, on April 6, 2010, Jamili wrote to Cheng, "do not worry, if we present 100 to 150pcs on time, then they will keep all 3 kpcs [kilo pieces, or 3000 pieces] for us."[37] Cheng was anxious to quickly supply another 1,000 as part of their ambition to supply 3,000. They were angling for more orders but Jamili reported that these discussions were going slowly.

Jamili added that the impact of sanctions was further complicating the situation. In the extended, verbatim copy of a section of the MSN Chat included below, Jamili attempted to explain the situation to Cheng, where, as discussed above, ECI was their codename for pressure transducers.[38] Cheng remained confident in gaining a new order and offered Jamili advice to increase the chances of a new order in a June 3, 2011 chat.

2011-06-03	12:41:45	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	what do you think of the current situation ?
2011-06-03	12:42:00	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	I am a little worrying about it

[37] MSN Chat record, as available in Government Exhibit 18, prosecutor's evidence.

[38] Government Exhibit 24.

2011-06-03	12:42:13	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	for what ?
2011-06-03	12:42:40	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	our politics in the world and hard sanction ?
2011-06-03	12:42:49	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	harder
2011-06-03	12:42:53	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	?
2011-06-03	12:43:22	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	what worries u in present situation ?
2011-06-03	12:43:25	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	?
2011-06-03	12:43:44	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	I mean ECI
2011-06-03	12:43:58	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	I don't know what the end user is thinking
2011-06-03	12:45:28	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	they bought 1000 pcs and their warehouse quantity is enought for their next 6 months projects
2011-06-03	12:45:50	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	and they have not teceived new purchasing project from their top management
2011-06-03	12:46:11	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	of course , if they will receive new order , we are their number 1 sorce
2011-06-03	12:46:21	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	ok, I see
2011-06-03	12:46:29	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	thank you for explanation
2011-06-03	12:46:42	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	but in future we do not know if still we will have current chance or not
2011-06-03	12:47:11	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	yes, the sanction is become harder

2011-06-03	12:47:23	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	as you can see, the exporting to Iran is become more difficult
2011-06-03	12:47:27	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	that is my only worry abiut the future , I tried a lot to convinvce them for another order of 1000 pcs but they did not accept
2011-06-03	12:47:34	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	you should explain what is happening to the end user
2011-06-03	12:47:47	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	tell them, they should cherish the chance to stock enough ECI
2011-06-03	12:48:13	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	recently the exporting to Iran is really changing
2011-06-03	12:48:21	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	you can report this new change to the end user
2011-06-03	12:48:33	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	maybe you can send a formal FAX to remind them
2011-06-03	12:48:43	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	remind them of the situation change
2011-06-03	12:48:56	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	in this way, maybe they can reconsider our advice
2011-06-03	12:51:32	Alex Cheng 成思海	Shahab Jamili-Nicaro Eng.Co.Ltd	just my personal advice, you make decision
2011-06-03	13:08:06	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	yes
2011-06-03	13:08:20	Shahab Jamili-Nicaro Eng.Co.Ltd	Alex Cheng 成思海	will do as your advice

In the end, however, they did not obtain another order for pressure transducers. This resulted from several developments, including their success in providing so many pressure transducers, changes in the centrifuge procurement organization, including the assassination of its head, Mostafa Ahmadi Roshan, in January 2012, possibly Eyvaz or the centrifuge program finding other suppliers offering cheaper prices, and finally the arrest of Hu in May 2012. Hu's arrest, in particular, ended MKS Shanghai as a source of pressure transducers for Cheng.

Cheng's Central Role

Cheng demonstrated his acumen as a strategic commodity trafficker by keeping Wang Ping loyal and directing Jamili to better protect their interests. In a March 10, 2010 blog posting in Chinese, Cheng clearly boasted of his efforts, but also showed his attempts to influence his Iranian customers to increase the chance of this illegal business prospering:[39]

> My customer was just executing my plans. Hehe~~because this business is really very special and very tricky! I must remind him to pay attention to every detail while talking to his customer [Eyvaz or gas centrifuge procurement department] in his country … For example, when he went to visit the end user, which sentence had to be said, when to say it, how to say it, what tone to use, how much to say and how much not to say, how to reply to the customer's response, what kind of smile to maintain, whether to explain further or simply shut up, etc. etc. all of these were meticulous to the extreme! I insisted that he should do these things completely according to my demands! Doing them correctly would save the building from crumbling down; any small misstep could cause complete failure and total loss of opportunity. For those friends who have watched "Qianfu,"[40] you should still remember the details in handling those dangerous moments; one mistake could lose the entire game and be doomed for eternity…."

As part of encouraging Jamili and the Iranian procurement office to speed up their decision of providing a new order, he even used the threat of war with the United States. On September 13, 2010, in the MSN Chat, he wrote to Jamili in a successive series of texts (with bullets added to ease reading):[41]

- It's time for you to discuss the new order with the end-user
- Time is important, not only for you, for me, for your end user, but also for your nation
- I personally believe THE WAR WILL BREAK OUT IN 2 YEARS
- and that will be the start of WORLD WAR THREE
- time is really precious
- and the war is not far away
- we already hear the steps of the big war!

Methods

This case helps to highlight several methods used by Iran and its network in procuring goods from the international marketplace, and in particular, from China:

---

[39] Government Exhibit 17. Translation by FBI.

[40] Qianfu, or Lurk, was an award-winning Chinese television series. The storyline, according to IMDb, was as follows: "While working in the KMT [Kuomintang, Taiwan] intelligence station in Tianjin, a Communist undercover agent achieved a series of incredible feats with the help of his stand-in wife."

[41] Government Exhibit 21.

1. Iranian agents formed an enduring relationship with Chinese businessman Alex Cheng, who was able to acquire sensitive goods repeatedly over a number of years.
2. Two Chinese intermediaries (Cheng and Wang Ping) created companies in China and Hong Kong that they used for the purposes of facilitating illicit trade in addition to their legitimate business.
3. Cheng built enduring (and corrupt) relationships with staff of MKS Shanghai, which had created an insider scheme to sell MKS pressure transducers and other MKS vacuum equipment illicitly for substantial profit. As part of this scheme, the staff conspired with Wang Ping who established fraudulent companies to help facilitate evading U.S., Chinese, and Hong Kong export controls.
4. The illicit procurement scheme appears to have evaded both company internal compliance procedures and due diligence of the U.S. export licensing system, along with any Chinese export controls.
5. Cheng often stressed the importance of building personal relationships with the suppliers.
6. The Iranian entities requested that the order be sourced in batches of 50-150 pressure transducers to avoid arousing suspicion of the United States and the supplier. But it should be noted that among European companies and governments, who have also been targeted by Iran's illegal schemes to acquire pressure transducers, by 2008 or 2009, any inquiry or request for a price quote involving more than 50 pressure transducers would trigger suspicion and further corporate and governmental investigations. However, in this case, MKS headquarters was confronted with an insider scheme that was actively deceiving them about the true end-users.
7. The Iranian intermediary expressed concern about a potential price increase by MKS of 8 percent, indicating that financial considerations are not secondary in relation to illicit procurement of vital equipment.
8. The business of conducting illicit commodity trafficking for Iran can be highly competitive among Iranian trading companies and expose foreign suppliers and agents to great legal risks.
9. Chinese intermediary (Cheng) shipped parcels to Nicaro, Eyvaz, or other consignees in Tehran using such standard shipping entities as DHL, indicating the difficulty authorities face in detecting illicitly obtained goods at the point of shipment.
10. Apart from the Shanghai Free Trade Zone, Hong Kong served as the major transshipment point before goods were sent to Iran.
11. Iranian intermediary (Jamili) allegedly used bank accounts located in the United Arab Emirates and Turkey to transfer payments to Cheng's Chinese bank so that he could pay the MKS Shanghai co-conspirators for the goods. Most of the payments to intermediary banks were T/T transfers, or bank wire transfers.

Supply beyond Pressure Transducers

In total, Cheng and Jamili procured and illegally exported 1,185 pressure transducers in eleven separate exports over a period of three years.[42] However, this is only part of what they sought or provided to Iran's gas centrifuge, other nuclear, and conventional military programs. Between 2005 and 2011, Cheng acquired many goods and described himself as Iran's "channel for getting … sensitive products."[43]

The other goods that he acquired or sought included:[44]

- Items for centrifuge cascade piping
- Components for Iran's heavy water production plant and heavy water reactor near Arak
- Titanium sheets and tubes
- Seamless stainless-steel tubes
- High strength aluminum tubing
- Carbon steel tubes coated with copper and yellow zinc
- Compressed natural gas tubes
- Vacuum valves
- Helium leak detectors
- Specialized hoses
- Stainless steel bellows
- Stainless steel flanges
- Mercury switches
- Rubber diaphragms
- High-speed camera

Cheng made these sales knowing that these parts were destined for Iran.[45] According to the Sentencing Memorandum:

> For each inquiry he received from Jamili for any parts…Cheng would investigate how the parts could be obtained in China, entice a distributor to sell it to him, lie about the end destination, pay the distributor, develop a safe shipping method to Iran, and take steps to conceal the parts being exported to Iran to avoid detection.[46]

Many of these goods and their significance are discussed in Volume 2 of this report.

[42] *Government's Sentencing Memorandum, USA vs Sihai Cheng*, p. 23.
[43] MSN Chat, April 4, 2012, 12:28:39. Government Exhibit 25.
[44] *Government's Sentencing Memorandum, USA vs Sihai Cheng*.
[45] Ibid, p. 8.
[46] Ibid, p. 13.

Last Word

According to the U.S. Attorney's Office of the District of Massachusetts, Cheng represented a significant threat to the United States:[47]

> Cheng gravely threatened the national security of the United States and other foreign countries by supplying pressure transducers to a WMD proliferator in Iran. These parts assisted Iran in its nuclear proliferation activities and helped Iran advance its nuclear weapons capabilities. Cheng blatantly and repeatedly violated U.S. laws and international sanctions, willingly supplied sensitive parts to Iran knowing they would be used for nuclear purposes, and invoked the threat of war between the United States and Iran as a means to increase his business.

[47] Ibid, p. 31.

Table 11.2. Summary of Shipments of MKS Pressure Transducers (PT)[48]

(more shipping data were included on the first four shipments than the others)

1st shipment-30 PT

722A13TGA2FJ; 30EA 5 pcs
722A11TGA2FJ; 500EA 20 pcs
722A01TGA2FJ; 260EA 5 pcs

Packing: 1 carton
Approximate shipping date of export from USA: April 24, 2009
Shipping date from Hong Kong: April 30, 2009

2nd shipment-61 PT

722A13TGA2FJ; 30EA 5 pcs
722A11TGA2FJ; 500EA 45 pcs
722A01TGA2FJ; 260EA 11 pcs

Packing: 2 cartons, with 30 and 31 pieces
DHL Number (from Hong Kong to Tehran): 2558873332 & 2915984875
Approximate shipping date of export from USA: June 10, 2009-June 11, 2009
Shipping date from Hong Kong: June 18, 2009

3rd shipment-38 PT

722A13TGA2FJ; 30EA 1 pcsf
722A11TGA2FJ; 500EA 27 pcs
722A01TGA2FJ; 260EA 10 pcs

Packing: 2 cartons, with 28 and 10 pcs
Approximate shipping date of export from USA: June 26-July 2, 2009
Shipping date from Hong Kong: July 18, 2009

4th shipment-56 PT

722A13TGA2FJ; 30EA 3 pcs
722A11TGA2FJ; 500EA 39 pcs
722A01TGA2FJ; 260EA 14 pcs

Packing: 2 cartons, with 27 and 29 pcs
Approximate shipping date of export from USA: July 22, 2009-July 27, 2009
Shipping date from Hong Kong: Aug. 25, 2009

[48] Government Exhibits 1 and 14.

5th shipment-100 PT
722A11TGA2FJ: 100 pcs
Approximate shipping date of export from the USA: April 21, 2010-April 26, 2010

6th shipment-100 PT
722A11TGA2FJ: 100 pcs
Approximate shipping date of export from the USA: July 8, 2010-July 23, 2010

7th shipment-100 PT
722A11TGA2FJ: 100 pcs
Approximate shipping date of export from the USA: September 3, 2010-September 14, 2010

8th shipment-100 PT
722B11TGA2FJ: 100 pcs
Approximate shipping date of export from the USA: September 19, 2010-October 13, 2010

9th shipment-100 PT
722B11TGA2FJ: 100 pcs
Approximate shipping date of export from the USA: October 18, 2010-October 25, 2010

10th shipment-100 PT
722B11TGA2FJ: 200 pcs
Approximate shipping date of export from the USA: December 2, 2010-January 20, 2011

11th shipment-100 PT
722B11TGA2FJ: 300 pcs
Approximate shipping date of export from the USA: February 22, 2011-March 30, 2011

Model	**Full-scale Reading**	**Number Exported**
722A13TGA2FJ	1000 torr	14
722A01TGA2FJ	1 torr	40
722A11TGA2FJ	10 torr	431
722B11TGA2FJ	10 torr	700
	Total	**1185**

Full-Scale Reading		**Number Exported**
1 torr		40
10 torr		1131
1000 torr		14
	Total	**1185**

Chapter 12. Iran's Procurement of High-Strength Carbon Fiber

Iran views the foreign acquisition of carbon fiber as a high priority. High-strength carbon fiber is desirable for military and uranium enrichment applications due to its strength, stiffness, and heat and chemical resistant properties. It has applications in aerospace vehicles, ballistic missiles, fighter jets, nuclear industries, and uranium centrifuge rotors. Thus, Iran uses carbon fiber in a range of nuclear, missile and military programs. However, its industry has not learned to make high-strength carbon fiber, despite some successes in making lower qualities of the material. Iran's supply situation is aggravated due to raw carbon fiber having a shelf life of only one to five years, where the latter is possible only if the fiber is stored carefully. Buying large quantities and stockpiling them for years is not an option.

As a result, Iranian procurement entities periodically seek carbon fiber from abroad. Since few countries will openly sell the material to Iran, it has to seek it illicitly. To acquire high-strength carbon fiber, Iran has established illicit procurement networks on several continents. It has made many attempts to procure such fiber for its centrifuge program, some of which have succeeded.[1] This chapter discusses two cases, a set of procurements from the United States, and another from China. Few companies make high-strength carbon fiber, making initial control easier. However, many others distribute carbon fiber after buying it from the primary suppliers, presenting a vulnerability that Iran has regularly exploited.

Background

Iran has sought many types of carbon fiber. A major manufacturer is Toray Industries, Inc., headquartered in Tokyo, Japan. Its T-series carbon fibers include T-800 carbon fiber, a type with applications in missile launchers, solid rocket motor shells, satellites, and spacecraft.[2] Centrifuge rotors typically use carbon fiber with a ranking above T-300. However, the lack of on-going supply of T-300 fiber has led Iran to seek the more common, but stronger, type T-700 for its centrifuges.

Iran's advanced centrifuges depend on a supply of carbon fiber. If it were to expand quantities of those centrifuges, as it has threatened to do, it would need a regular supply involving many metric tonnes of carbon fiber.

For several years, Iran has been researching and developing a range of advanced centrifuges, such as the IR-2m, IR-4, IR-5, IR-6s, IR-6, IR-7, and IR-8 centrifuges.[3] All of them require carbon

[1] See for example: David Albright, Andrea Stricker, and Houston Wood, *Future World of Illicit Nuclear Trade: Mitigating the Threat* (Washington, D.C.: Institute for Science and International Security, July 29, 2013), http://isis-online.org/isis-reports/detail/future-world-of-illicit-nuclear-trade-mitigating-the-threat/

[2] "The difference between T700 and T800 carbon fibers," in *Cncarbonfiber, Inc*., 2019,http://www.cncarbonfiber.com/the-difference-between-t700-and-t800-carbon-fibers/

[3] "Iran's Long-Term Centrifuge Enrichment Plan: Providing Needed Transparency," *Institute for Science and International Security*, April 25, 2019,

fiber in their rotor assemblies. Figure 12.1 shows a carbon fiber bellows for an Iranian advanced centrifuge. It is believed to use T-700 grade carbon fiber in its centrifuge rotors. It is unclear what grade it uses to make carbon fiber bellows. About 1,000 IR-2m centrifuges were deployed at the Natanz Fuel Enrichment Plant prior to the Iran nuclear deal in 2015. They were put into storage under the deal.

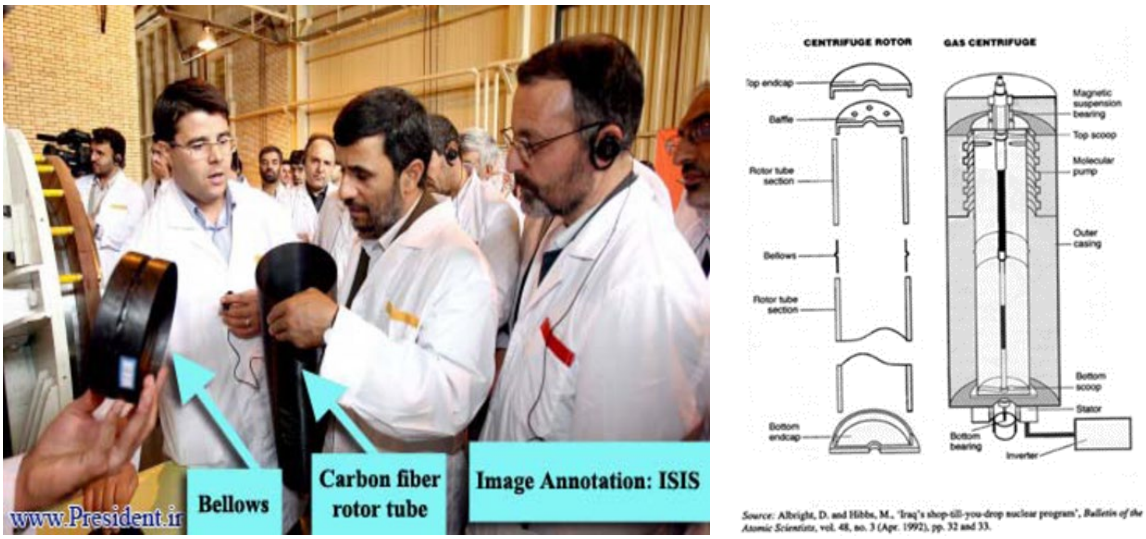


Figure 12.1. Then President Mahmoud Ahmadinejad holds a carbon fiber rotor tube at the Natanz enrichment site; visible is also a centrifuge bellows, which appears to have been made from carbon fiber. A schematic of a two-rotor tube assembly connected by a bellows is shown at right. Credit for left photo: Iran's Presidential web site.

Case 12.1: Iranian Procurement Network Obtained High-Performance Carbon Fiber Materials from the United States

On July 16, 2019, the Department of Justice released an indictment of Ali Reza Shokri (aged 61), Behzad Pourghannad (65), and Farzin Faridmanesh (48), Iranian citizens who are accused of facilitating an illicit procurement scheme to obtain carbon fiber materials for Iran.[4] Shokri and Pourghannad reside in Iran, and Faridmanesh resides in Iran and the Republic of Georgia. According to the LinkedIn profile of Behzad Pourghannad, he served as the Chairman of the Board and technical manager for Alborz Microsystems, an industrial automation company for water, waste management, sewage, and industrial electricity.[5] This case follows a separate indictment released by the Department of Justice on October 24, 2012, which charged Hamid

http://isis-online.org/isis-reports/mobile/irans-long-term-centrifuge-enrichment-plan-providing-needed-transparency

[4] *Indictment: United States of America v Ali Reza Shokri, Behzad Pourghannad, and Farzin Faridmanesh,* 13 CR 507 (2019), Filed July 11, 2013. Available at www.Pacer.gov.

[5] "Behzad Pourghannad," *LinkedIn,* August 27, 2019, https://www.linkedin.com/in/behzad-pourghannad-46aa6154/

Reza Hashemi (52) and Murat Taskiran (age not given) for participating in the same scheme to obtain carbon fiber materials for Iran.[6] Hashemi is a dual U.S. and Iranian citizen and resides in Iran. Taskiran is a Turkish citizen and resides in Turkey. Shokri and Hashemi own a company in Tehran that was the origin and recipient of the alleged carbon fiber orders. An analysis of available public records in the United States and in Iran, as well as a LinkedIn profile, reveals that an individual with the same name as Hashemi is the managing director of Arian Sadeh (aka HB Composite), an oil and gas pipes and fittings manufacturer located in Tehran, Iran.[7]

The indictments cite the same incidents and evidence.[8] All of the accused face charges of violating the U.S. International Emergency Economic Powers Act (IEEPA).[9] Due to the nature of the commodities and their destination, it is possible the materials were used by or intended for Iranian nuclear, missile, or military programs that are subject to U.S. and international embargoes.

As a dual-use good, certain types of carbon fiber are subject to export controls through the Department of Commerce; it is also tightly controlled for export by the European Union and many other countries' laws. UN Security Council resolutions in place prior to 2015 prohibited high-strength carbon fiber exports to Iran; Resolution 2231 (2015) still requires Iran to procure such goods through a procurement channel headquartered at the United Nations.

The Iranian network allegedly sought HexTow IM7 carbon fiber, an intermediate modulus aerospace-grade carbon fiber, which is manufactured by Hexcel Corporation, headquartered in Stamford, Connecticut.[10] This network also sought T-300, T-700, T-800, and T-1000 carbon fiber, which is manufactured by Toray Industries, Inc., as stated, headquartered in Tokyo, Japan, but sold through its locations and distributors in the United States.

Hashemi was arrested on December 1, 2012, while arriving at John F. Kennedy Airport in New York, and planning to visit a supplier of industrial equipment. Hashemi pleaded guilty to the charges.[11] Pourghannad was arrested in Germany on May 3, 2017, and extradited to the United States on July 15, 2019. According to court records, Pourghannad has pleaded not guilty

---

[6] *Indictment: United States of America v Hamid Reza Hashemi and Murat Taskiran,* 12 CR 804 (2012), Filed October 24, 2012. Available at www.Pacer.gov.

[7] "Hamid R. Hashemi," *LinkedIn,* August 27, 2019, https://www.linkedin.com/in/hamid-r-hashemi-42037138/

[8] Based on the documents and the corroborating information available in public records, unnamed co-conspirator-1 (CC-1) in the Shokri, Pourghannad and Fraidmanesh indictment is likely Hashemi. Another un-named co-conspirator-2 (CC-2) in the Shokri, Pourghannad, and Fraidmanesh indictment is likely Taskiran.

[9] Shokri, Pourghannad, and Fraidmanesh are indicted on three counts of Conspiracy to Violate IEEPA, which carries a 20-year maximum sentence, and two counts of violation and attempt to violate the IEEPA, which also carries a 20-year maximum sentence. Hashemi is indicted on one count of conspiracy to violate IEEPA, and two counts of IEEPA violations, facing 60 years in prison. Taskiran is indicted on one count of conspiracy to violate IEEPA, and one count of IEEPA violation, facing 40 years in prison.

[10] "HexTow IM7 Carbon Fiber: Product Data Sheet," in *Hexcel*, 2019, https://www.hexcel.com/Resources/DataSheets/Carbon-Fiber

[11] "Factbox: Iranians Facing Trial or Imprisoned in U.S. for Sanctions-Busting," Reuters, January 12, 2016, https://www.reuters.com/article/us-iran-nuclear-usa-prisoners-factbox-idUSKCN0UR02820160113

to the charges.[12] The other alleged co-conspirators remain at large. The cases are being prosecuted by the U.S. District Attorney for the Southern District of New York. The court has yet to issue rulings on the cases.

The Scheme

The indictments state that between 2007 and 2013, Shokri, Pourghannad, Faridmanesh, along with Hashemi and Taskiran, were allegedly involved in Iran's efforts to illegally procure many tons of IM7 carbon fiber, and T-300, T-700, T-800, and T-1000 Toray carbon fiber from a U.S. broker of carbon fiber. The broker/supplier resided in Orange County, New York. Following purchase requests from Taskiran, Shokri, and Hashemi, an unnamed European individual would allegedly contact the U.S. broker/supplier. The unnamed individual operated businesses in Europe between 2007 and 2011 that allegedly "procured carbon fiber on behalf of various companies, including from locations in the United States." He or she also operated a company or companies or transit point(s) in Dubai, United Arab Emirates (UAE). The U.S. broker/supplier would allegedly arrange the purchase and export the carbon fiber to the unnamed individual in Europe or to unnamed European countries, and then, using a European freight forwarder, the individual in Europe would allegedly have the consignments transshipped to Iran via Dubai, UAE, Tbilisi, Georgia, or Turkey. The consignments sent via Georgia or Turkey used the companies owned and operated by Faridmanesh and Taskiran, respectively. In Iran, they were received by the company operated by Shokri and Hashemi in Tehran, Iran.

One shipment in 2008, which went via Dubai, appears to have been successful in reaching Iran. It is unclear whether a second shipment that year, discussed for transshipment via Turkey, made it to Iran. A third shipment, in 2009, was seized by officials as it was attempted to be transshipped through the United Kingdom to Dubai. Fourth and fifth major shipments in 2013 appear to have been successful in reaching Iran via Tbilisi, Georgia. The network also allegedly discussed illicitly shipping goods via Pakistan.

According to the press release accompanying the most recent indictment, Iranian company owner Pourghannad served as the financial guarantor for the carbon fiber purchases, while Faridmanesh served as the facilitator for the carbon fiber transshipments.[13] A guarantor may have been necessary, as other cases show, because the Iranian end-users could be slow in making payments, relative to when payments had to be made to the supplier and shippers. The Iranian end-user often wanted to pay once the goods arrived in Iran, rather than before or upon shipment, as is customary in legitimate business where seizure by customs authorities is a small risk.

---

[12] *Plea Entry: United States of America v Ali Reza Shokri, Behzad Pourghannad, and Farzin Faridmanesh,* 13 CR 507 (2019), Filed July 11, 2013. Available at https://www.pacer.gov/

[13] U.S. Department of Justice, "Department of Justice Announces Extradition of Iranian National and Unsealing of Charges against Two Other Men for Exporting Carbon Fiber from the United States to Iran," July 16, 2019, https://www.justice.gov/opa/pr/department-justice-announces-extradition-iranian-national-and-unsealing-charges-against-two#_ftn1

The indictment indicated that the unnamed individual in Europe assisted in falsely labeling the carbon fiber shipments as "acrylic," or "polyester" in order to disguise their true nature. All of the actors in the scheme appear to have been aware of the export restrictions on carbon fiber at the time of the shipments and attempted purchases.

Since the Toray carbon fiber was not U.S.-origin, but manufactured in Japan, this case shows that the United States can also be a diversion point.

Transactions

2008 IM7 Carbon Fiber Transactions

Procurement #1

Between 2007 and 2008, a time when there was far less scrutiny over Iran's illicit procurements, Shokri and Taskiran allegedly arranged with the U.S. broker/supplier to purchase and illegally ship IM7 carbon fiber to the Iranian company. On November 21, 2007, Taskiran e-mailed the U.S. broker/supplier seeking IM7 carbon fiber. On December 5, 2008, the U.S. broker/supplier requested the assistance of the unnamed individual in Europe to facilitate the shipment and act as "their direct contact." On that same day, Taskiran and the unnamed individual in Europe initiated contact via e-mail and began to facilitate the alleged IM7 carbon fiber shipment. In the e-mail, the unnamed individual in Europe informed Taskiran that the desired carbon fiber was produced at facilities located in Atlanta, Georgia. On January 24, 2008, Taskiran informed the unnamed individual that the IM7 carbon fiber shipment, after initial export, would be resold to a company based in Tehran, Iran, for use in "CGN (compressed natural gas) tank production," a somewhat common cover story. Taskiran and the unnamed individual also discussed an "opportunity to sell all kind[s] of US products…on the Turkish Market." On January 25, 2008, Taskiran identified the recipient company based in Tehran, Iran, as the Iranian company owned by Shokri and Hashemi.

Nearly a month later, on February 21, 2008, Taskiran sent the unnamed individual proof of a wire transfer for $28,170 and a request to "pls proceed [with] the [carbon fiber] shipment in US." On February 22, 2008, the unnamed individual in Europe sent $28,170 via wire transfer from Europe to the U.S. bank account held by the U.S. broker/supplier. On March 10, 2008, the unnamed individual in Europe informed Taskiran that a company located in Dubai, UAE, owned by him or her, would serve as a transshipment point and that his or her forwarding customs agent would facilitate the transshipment. He or she also noted that the Iranian end-user needed to pay for the service. In March 2008, the IM7 carbon fiber shipment allegedly left the United States for an unnamed European country. In mid-March 2008, from Europe, the shipment was allegedly transshipped through Dubai, UAE to the Iranian company operated by Shokri and Hashemi (Figure 12.2 shows the path of the procurement and shipment routes for this transaction).

On June 4, 2008, Taskiran and Hashemi discussed via e-mail payment for the carbon fiber shipment. In the same e-mail, Taskiran acknowledged that international restrictions forced the shipment to be sent through Europe, rather than directly to Iran. Also, on June 5, 2008, Taskrian informed the unnamed individual in Europe that Hashemi and Shokri are business partners and that "[Shokri] has the money and he take[s] care [of] financial issues and [Hashemi] has knowledge and experience about composites and he take[s] care of technical issues."

Following this correspondence, Taskiran e-mailed Hashemi and Shokri expressing his concerns about shipping restrictions and stating that he had directed the IM7 carbon fiber shipment through Europe. He also included a request to "make payment… very PROMPTLY." In subsequent e-mails between Hashemi and Taskiran, where Shokri is copied, Hashemi confirmed that the remaining balance from the shipment transaction would be sent to Taskiran as payment to "settle the account and KEEP YOU [Taskiran] HAPPY!!!," along with a request for Taskiran's bank account information.

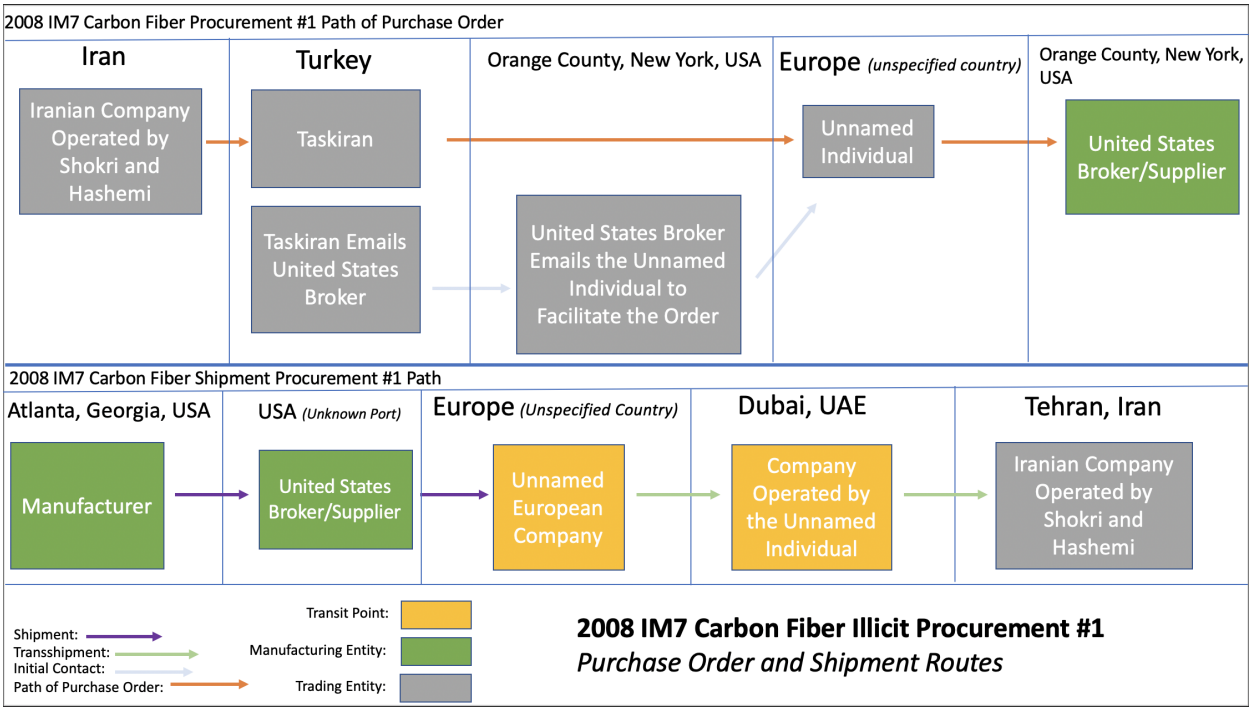


Figure 12.2. Procurement #1 - paths of purchase orders and shipments allegedly used by the conspirators in 2008 to obtain IM-7 carbon fiber materials. Note: it is unclear whether the U.S. broker/supplier physically shipped the items him or herself. One interpretation of the shipment route is indicated in the diagram.

Procurement #2

The Hashemi and Taskiran indictment indicates that on June 12, 2008, the unnamed individual in Europe and Taskiran in Turkey discussed a different shipment of carbon fiber, to be shipped

from the United States to Turkey and on to Tehran, Iran (See Figure 12.3). It is unknown if the unnamed individual contacted the same United States based supplier/broker for this procurement. On June 12, 2008, Taskiran e-mailed the unnamed individual in Europe asking if the materials could be transshipped through Pakistan in order to reduce the shipping cost of the carbon fiber. On June 18, 2008, Taskiran and the unnamed individual discussed how the carbon fiber shipment would be transshipped through Turkey and that the price of the carbon fiber could not be lowered. One month later, on July 19, 2008, the unnamed individual in Europe e-mailed Hashemi a specification sheet with information on many types of carbon fiber, as well as a price quote for $12,000 for IM7 carbon fiber priced at 70 Euros/kilogram (kg). Neither indictment indicated the final outcome of this order.

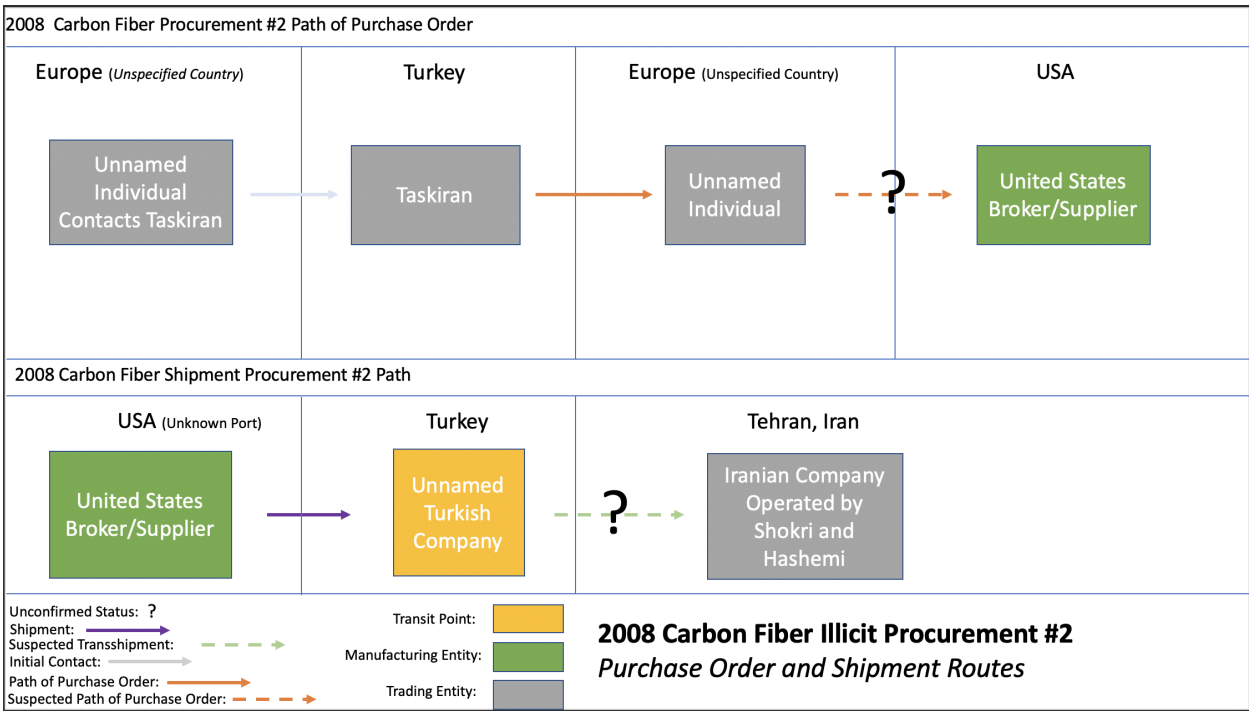


Figure 12.3. Procurement #2 - paths of purchase orders and shipments allegedly attempted for use by the conspirators in 2008 to obtain carbon fiber materials.

2009 Carbon Fiber Material Transaction

Procurement #3

In mid-2009, Shokri, Pourghannad, and Hashemi allegedly attempted to facilitate a shipment of 1,500 kg (ultimately, 3,095 kg) of carbon fiber material via transshipment through the United Kingdom and the UAE to Iran, using DHL shipping. On May 6, 2009, the unnamed individual e-mailed Hashemi with price quotations for an unspecified type of carbon fiber priced at 75 Euros/kg. On the same day, Hashemi e-mailed the unnamed individual and stated that tests were carried out on the samples he or she had sent. Nearly two weeks later, Hashemi responded with a request to process a shipment for 1,500 kg of an unspecified type of carbon

fiber material for delivery to Tehran, Iran, presumably to the Iranian company. On May 27, 2009, Hashemi e-mailed the unnamed individual a proposed contract for a shipment of 1,500 kg of an unspecified type of carbon fiber material, as well as an office fax number. The contract listed Shokri as the purchaser. That same day, the unnamed individual e-mailed Pourghannad an attachment entitled, "Final Contract for Mr. Shokri.doc." Again, on May 27, 2009, the unnamed individual e-mailed Pourghannad the signed final copy of the contract containing Shokri's signature.

On July 6, 2009, the unnamed individual arranged a wire transfer of $43,738.38, apparently a partial payment, from Europe to the U.S. bank account of the U.S. supplier. The Hashemi and Taskiran indictment indicates that following this correspondence, an order for 3,095 kg of carbon fiber was shipped to a company located in the United Kingdom, with a final destination of Tehran, Iran. It is unclear in the indictment if the manufacturer of the carbon fiber arranged for the shipment or if the broker did. On July 29, 2009, a representative of the unnamed United Kingdom company e-mailed the unnamed individual, "We [unnamed United Kingdom Company] can ship to Dubai with no problem." However, the UK authorities subsequently seized the shipment before it left for Iran (see Figure 12.4).

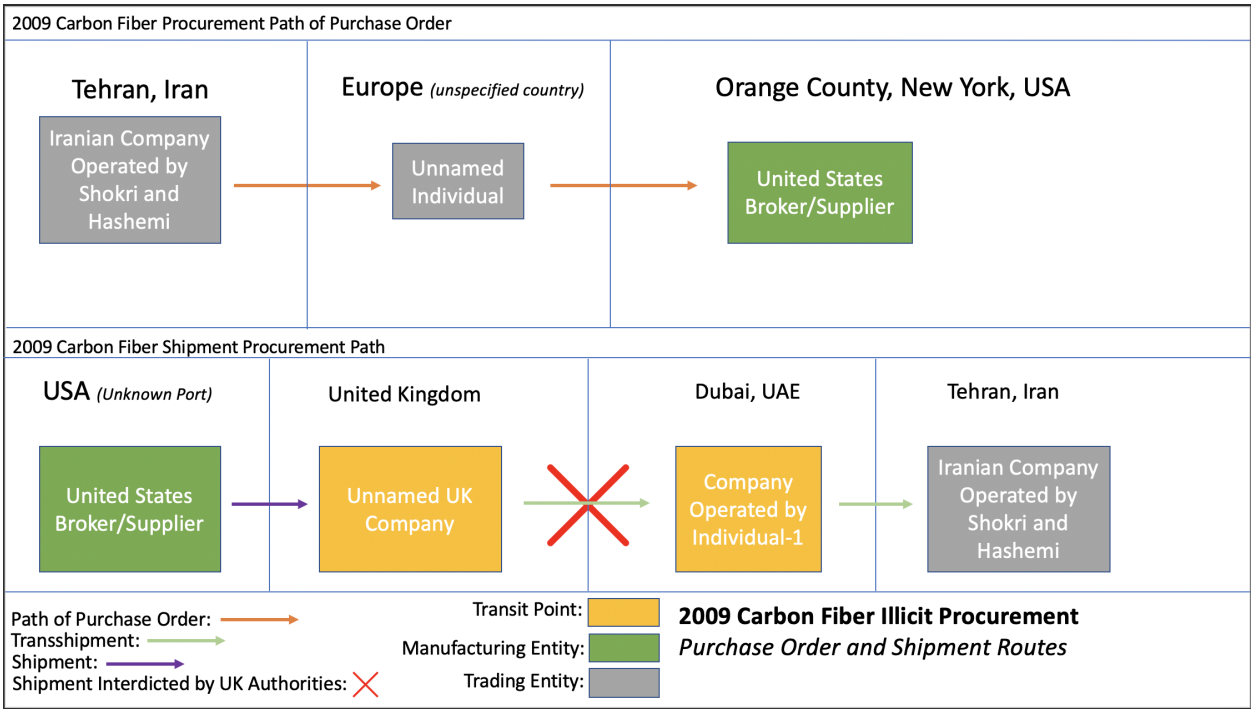


Figure 12.4. Procurement #3 - Path of purchase order and shipment allegedly used by the conspirators in 2009 to obtain unspecified carbon fiber materials.

2013 T-300, T-700, T-800, T-1000, and IM-7 Carbon Fiber Transactions

Procurements #4 and #5

According to the indictment, between January and July 2013, Shokri, Pourghannad, and Faridmanesh allegedly worked to circumvent U.S. export controls by seeking to purchase between 500 kg and 5 tons of T-300, T-700, T-800, T-1000, carbon fiber and IM7 carbon fiber from a United States broker/supplier via transshipment through Tbilisi, Georgia, to Tehran, Iran (see Figure 12.5). During this time, two purchase contracts were signed between these three co-conspirators and the unnamed individual. The indictment indicates the two consignments were allegedly shipped together.

The carbon fiber was likely made in Japan and shipped to the distributors in America.

On January 2, 2013, Shokri contacted the unnamed individual via voice-over-internet-protocol (VOIP) to discuss the price for an undisclosed quantity of T-700 carbon fiber. Two weeks later, on January 14, 2013, Shokri again contacted the unnamed individual to discuss purchasing 500 kg of T-700 carbon fiber each week, up to a total of 5 tons of material, and asked for an invoice for the purchase. One week later, on January 21, 2013, Pourghannad and the unnamed individual discussed the cost of transporting the carbon fiber shipment to Iran.

In March 2013, Shokri and the unnamed individual began discussing a second purchase contract for T-800 and T-1000 carbon fiber. In April 2013, Pourghannad followed up with the unnamed individual and provided a contract (Contract-1 in the indictment) for 5 tons of T-700 carbon fiber to be delivered to Tehran, Iran. The contract listed Shokri as the purchaser and the unnamed individual as the seller of the 5 tons of T-700 carbon fiber. On April 11, 2013, Shokri provided the unnamed individual a signed copy of the contract, as well as a proposed second contract (Contract-2 in the indictment) for "thousands of kilograms of T-800 and T-1000 carbon fiber," again for delivery to Tehran, Iran. On April 16, 2013, Faridmanesh and Pourghannad had a VOIP conversation with the unnamed individual, where Faridmanesh indicated that the T-700 carbon fiber shipment in Contract-1 would be transshipped through Tbilisi, Georgia, to Tehran, Iran. On April 21, 2013, Shokri provided the unnamed individual with signed copies of Contract-1 and Contract-2.

The indictment stated that on May 3, 2013, Faridmanesh and the unnamed individual discussed falsifying the carbon fiber shipping labels to state, "something other than 'carbon fiber.'" On May 9, 2013, Faridmanesh and the unnamed individual discussed altering the carbon fiber shipment labels to state the contents as "acrylic," and "polyester." Pourghannad then e-mailed the unnamed individual a bank guarantee for the purchase in Contract-1. On June 26, 2013, the unnamed individual confirmed to Shokri that the carbon fiber shipments set forth in Contract-1 and Contract-2 would ship from a "Manhattan Port in approximately 10 days." In the same conversation, the unnamed individual confirmed that he or she "removed all of the labels for T-700, [T]800, [T]300, IM7, [T]1000 [carbon fiber]," and "put acrylic on it [the shipment label]." The unnamed individual then acknowledged that "acrylic is something that does not require a

permit, an export license." The unnamed individual also acknowledged that he or she was aware that carbon fiber shipments to Iran are subject to U.S. sanctions and export controls.

On the same day, the unnamed individual had this same discussion with Pourghannad and Faridmanesh, each in separate conversations. During these conversations, the unnamed individual confirmed that he or she had falsified the carbon fiber shipment labels to read "acrylic," and that he or she was aware that U.S. sanctions restrict the export of carbon fiber to Iran.

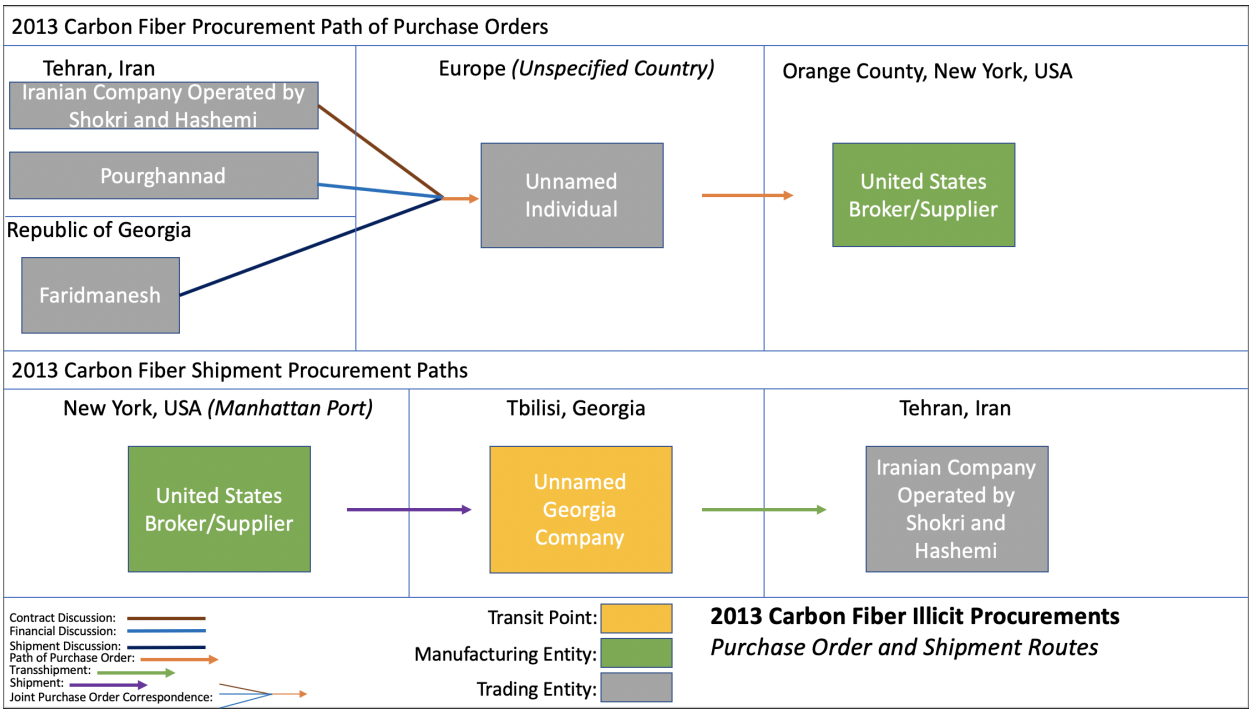


Figure 12.5. Procurements #4 and #5 - Paths of purchase orders and shipments allegedly used by the conspirators in 2013 to obtain two consignments of T-300, T-700, T-800, T-1000, and IM-7 carbon fiber materials.

Case 12.2: Seizure of Carbon Fiber Shipment from China to Iran in Bahrain

On August 29, 2014, the U.S. Department of State announced the addition of the Iranian entity Jahan Tech Rooyan Pars for its involvement in illicit procurement of WMD-related goods under then U.S. sanctions against Iran (under Executive Order 13382).[14] The State Department press release indicated that between 2010 and 2013, Jahan Tech Rooyan Pars attempted to procure "high-strength carbon fiber from Asia-based suppliers, some of which is controlled for export pursuant to the Nuclear Suppliers Group (NSG) Guidelines and is proscribed for export to Iran by UNSCR 1737."

[14] U.S. Department of State, "Additional Sanctions Imposed by the Department of State Targeting Iranian Proliferators," Press Release, August 29, 2014, https://2009-2017.state.gov/r/pa/prs/ps/2014/231159.htm

One such procurement was seized by Bahraini customs authorities in November 2010. The shipment was seized on the basis of an intelligence tip that it was suspected of containing certain goods from China banned for export to Iran under UN Security Council resolutions. Upon inspection of the shipment, officials discovered 28 packages of carbon fiber with a mass of 1,106 kilograms. Bahraini officials concluded that the carbon fiber met the control thresholds for dual-use goods (see INFCIRC/254/Rev.7/Part 2), which would constitute a violation of relevant resolutions.[15]

The shipper in China was listed as Shenzhen Sinotech Logistics, Shanghai Branch Co. Ltd. This is an international shipping company, not the original supplier in China. The importer listed on the Air Waybill was Science and Technology Park in Shiraz, Iran. The listed address matched that of Jahan Tech Rooyan. The departure airport is listed as Kuala Lumpur International Airport in Malaysia (apparently the first transit point) and Bahrain International Airport (BAH) is listed as intermediate on the route to Imam Khomeini international airport (IKA) in Tehran. "SZX IAK" at the top of the document appears to indicate the whole journey of the consignment, as SZX is the airport code for Shenzhen Airport (see Figure 12.6).

Jahan Tech Rooyan was also designated due to its attempted or actual procurement of 100,000 highly specialized ring magnets with specifications relevant to use in centrifuges. The amount sought would have been adequate to outfit 50,000 centrifuges. The ring magnet dimensions and tolerances matched those of Iran's IR-1 centrifuge. The inquiries occurred in late 2011 via a Chinese commercial website. The attempted ring magnet procurement by Jahan Tech Rooyan Pars was first publicly revealed by the Institute, which obtained a copy of the inquiry for the specialized ring magnets, analyzed it, and determined that the specifications matched the ring magnets for Iran's IR-1 centrifuges.[16] The Institute's report was covered in a February 2013 *Washington Post* story, which was mentioned in the State Department press release.[17] Additional information about this case was published in another Institute review of this case.[18]

The public revelation in the State Department press release that Jahan Tech Rooyan Pars was involved in seeking both high-strength carbon fiber and ring magnets demonstrates that this company was seeking various sensitive goods. The evidence indicates that in fact this company

---

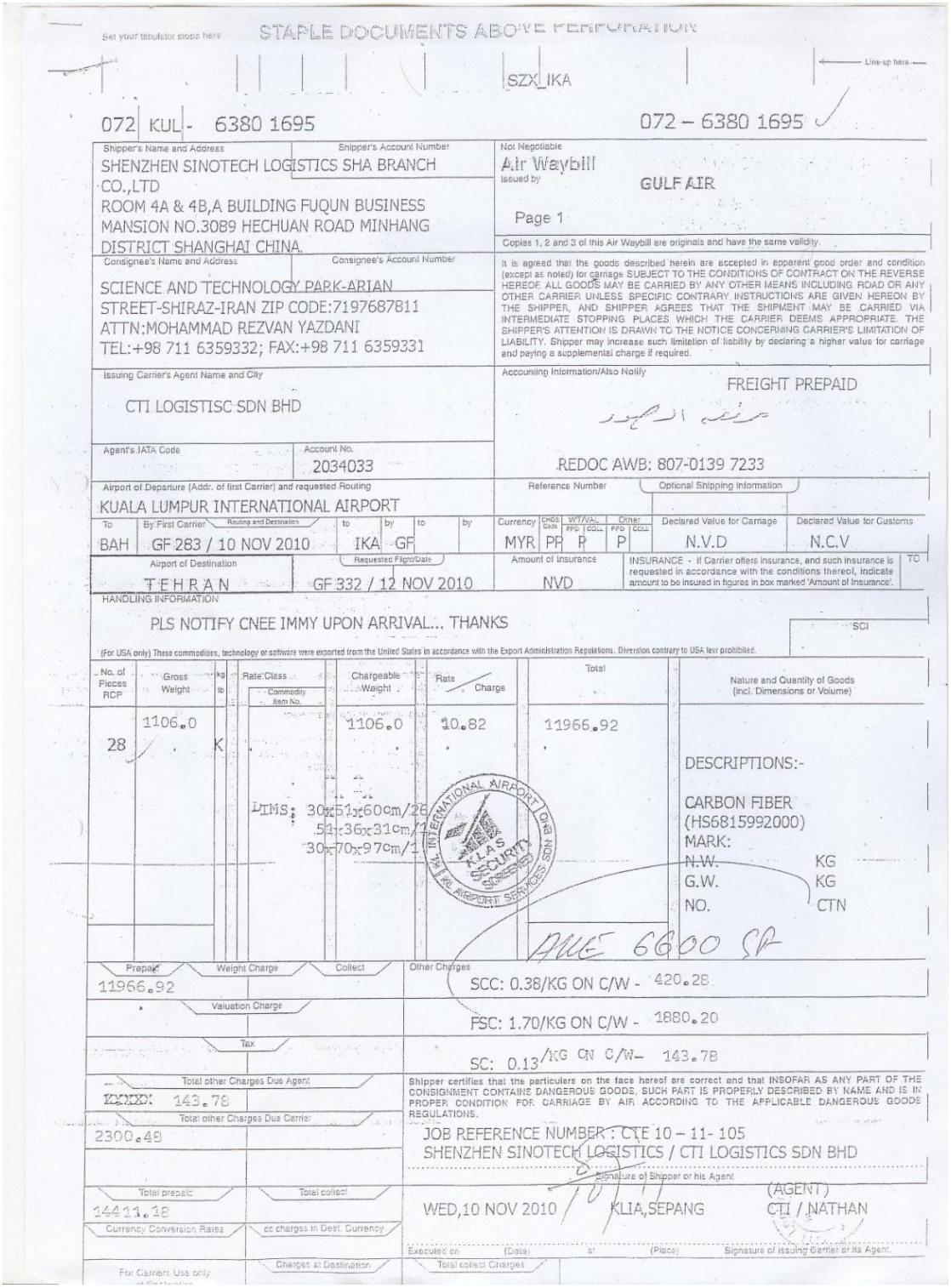
[15] United Nations Panel of Experts on Iran, *Final Report of the Panel of Experts established pursuant to Resolution 1929 (2010)*, S/2013/331, June 5, 2013, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2013_331.pdf

[16] David Albright, "Ring Magnets for IR-1 Centrifuges," *Institute for Science and International Security,* February 13, 2013, http://isis-online.org/uploads/isis-reports/documents/iran_ring_magnet_13Feb2013.pdf

[17] Joby Warrick, "Iranian Buying Spree Raises Concerns about Major Expansion of Nuclear Capacity," *The Washington Post*, February 13, 2013, http://www.washingtonpost.com/world/national-security/iranian-buying-spree-raises-concerns-about-major-expansion-of-nuclear-capacity/2013/02/13/2090805c-7537-11e2-8f84-3e4b513b1a13_story.html

[18] Albright, "Preventing the Suppression of Uncomfortable Truths on Iran's Nuclear Program," *Institute for Science and International Security,* March 7, 2013, http://isis-online.org/isis-reports/detail/preventing-the-suppression-of-uncomfortable-truths-on-irans-nuclear-program/8

was acting to procure illegally sensitive centrifuge-related goods for the Iranian centrifuge program.



STAPLE DOCUMENTS ABOVE PERFORATION

SZX IKA

072 KUL - 6380 1695

072 – 6380 1695

Shipper's Name and Address: SHENZHEN SINOTECH LOGISTICS SHA BRANCH CO.,LTD ROOM 4A & 4B,A BUILDING FUQUN BUSINESS MANSION NO.3089 HECHUAN ROAD MINHANG DISTRICT SHANGHAI CHINA.

Not Negotiable
Air Waybill
Issued by: GULF AIR

Page 1

Copies 1, 2 and 3 of this Air Waybill are originals and have the same validity.

Consignee's Name and Address: SCIENCE AND TECHNOLOGY PARK-ARIAN STREET-SHIRAZ-IRAN ZIP CODE:7197687811 ATTN:MOHAMMAD REZVAN YAZDANI TEL:+98 711 6359332; FAX:+98 711 6359331

It is agreed that the goods described herein are accepted in apparent good order and condition (except as noted) for carriage SUBJECT TO THE CONDITIONS OF CONTRACT ON THE REVERSE HEREOF. ALL GOODS MAY BE CARRIED BY ANY OTHER MEANS INCLUDING ROAD OR ANY OTHER CARRIER UNLESS SPECIFIC CONTRARY INSTRUCTIONS ARE GIVEN HEREON BY THE SHIPPER, AND SHIPPER AGREES THAT THE SHIPMENT MAY BE CARRIED VIA INTERMEDIATE STOPPING PLACES WHICH THE CARRIER DEEMS APPROPRIATE. THE SHIPPER'S ATTENTION IS DRAWN TO THE NOTICE CONCERNING CARRIER'S LIMITATION OF LIABILITY. Shipper may increase such limitation of liability by declaring a higher value for carriage and paying a supplemental charge if required.

Issuing Carrier's Agent Name and City: CTI LOGISTISC SDN BHD

Accounting Information/Also Notify: FREIGHT PREPAID

Agent's IATA Code: Account No. 2034033

REDOC AWB: 807-0139 7233

Airport of Departure (Addr. of first Carrier) and requested Routing: KUALA LUMPUR INTERNATIONAL AIRPORT

Reference Number | Optional Shipping Information

To	By First Carrier	Routing and Destination	to	by	to	by	Currency	CHGS Code	WT/VAL PPD	WT/VAL COLL	Other PPD	Other COLL	Declared Value for Carriage	Declared Value for Customs
BAH	GF 283 / 10 NOV 2010		IKA	GF			MYR	PP	P		P		N.V.D	N.C.V

Airport of Destination	Requested Flight/Date	Amount of Insurance	INSURANCE - If Carrier offers insurance, and such insurance is requested in accordance with the conditions thereof, indicate amount to be insured in figures in box marked 'Amount of Insurance'.	TC
TEHRAN	GF 332 / 12 NOV 2010	NVD		

HANDLING INFORMATION

PLS NOTIFY CNEE IMMY UPON ARRIVAL... THANKS

SCI

(For USA only) These commodities, technology or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to USA law prohibited.

No. of Pieces RCP	Gross Weight	kg lb	Rate Class / Commodity Item No.	Chargeable Weight	Rate / Charge	Total	Nature and Quantity of Goods (incl. Dimensions or Volume)
28	1106.0	K		1106.0	10.82	11966.92	DESCRIPTIONS:- CARBON FIBER (HS6815992000) MARK: N.W. KG G.W. KG NO. CTN

DIMS: 30x51x60cm/25
51x36x31cm/1
30x70x97cm/1

KLIA SECURITY SCREENED

AWE 6600 SP

Prepaid	Weight Charge	Collect	Other Charges
11966.92			SCC: 0.38/KG ON C/W - 420.28
	Valuation Charge		FSC: 1.70/KG ON C/W - 1880.20
	Tax		SC: 0.13/KG ON C/W - 143.78
	Total other Charges Due Agent		Shipper certifies that the particulars on the face hereof are correct and that INSOFAR AS ANY PART OF THE CONSIGNMENT CONTAINS DANGEROUS GOODS, SUCH PART IS PROPERLY DESCRIBED BY NAME AND IS IN PROPER CONDITION FOR CARRIAGE BY AIR ACCORDING TO THE APPLICABLE DANGEROUS GOODS REGULATIONS.
	Total other Charges Due Carrier		JOB REFERENCE NUMBER : CTE 10 – 11- 105 SHENZHEN SINOTECH LOGISTICS / CTI LOGISTICS SDN BHD
			Signature of Shipper or his Agent
Total prepaid	Total collect		
			WED,10 NOV 2010 KLIA,SEPANG (AGENT) CTI / NATHAN
Currency Conversion Rates	cc charges in Dest. Currency		Executed on (Date) at (Place) Signature of Issuing Carrier or its Agent
For Carrier Use only	Charges at Destination		Total collect Charges

2300.48

143.78

14411.18

Figure 12.6. Air Waybill of seized high-strength carbon fiber in Bahrain, showing Iranian recipient in Shiraz, Iran.

Section V. Findings and Recommendations

Chapter 13. Methods used to Defeat Strategic Trade Controls and their Warning Signs

Detecting and preventing illicit trade is enormously challenging. However, knowing how it occurs can help in developing warning signs that help counter it. The cases show that commodity trafficking can be stopped when suppliers, banks, and shippers are vigilant and follow a straightforward set of strategic trade control policies. Governments also can benefit from case assessments to develop a deeper understanding of the trends and threats of illicit trade.

Depending on their day-to-day work, resources, mandate, authority, and experience, authorities and private sector officials engaged in detecting and preventing illicit procurement have differing abilities to identify signs of banned activity. Moreover, the numerous persons and entities directly or indirectly involved in an export transaction may include, but are not limited to: suppliers (manufacturers and distributors), trading companies, brokers, sales managers, compliance officers, licensing officials, customs and other border control agents, intelligence, government trade, and financing analysts, banking officials, shipping companies, freight forwarders, transportation providers, logistics managers, ship or company registries, classification service providers, insurance companies, port and airport operators, industry associations, and banks and other financial institutions, including loan providers and exchange houses.

All involved parties must be aware of methods and warning signs and understand that together they act as a net to detect and prevent illicit procurements from successfully making their way to proliferant states. For example, an illicit procurement network's method to deceive one authority can be a tip-off for another. A cash payment may circumvent financial compliance officers in an electronic transfer, but may cause suspicion by the supplier. A circuitous shipping route may deceive customs officials, but alert a carrier. A trading company may hide the actual end-user, but still inadvertently alert the supplier country's licensing agency to the possibility of illicit activity. A free trade zone as final destination may cut out customs controls, but create extra due diligence by a freight forwarder. All these entities are connected and perform a collective task of detection and prevention.

It is the government's responsibility to reach out and educate industry, shipping, and financial sectors regarding national laws, regulations, often-used methods by illicit procurement networks and proliferant states, and specific tips about a dangerous sale. At the same time, these entities serve to raise the awareness of governments about both the tactics of traffickers and states seeking goods illegally, as well as a deeper understanding of the underlying programs needing those goods. Governments also benefit by learning the trends of illicit procurements and the successes and failures of controls.

The case studies in this report allow for a deeper understanding of the methods and tactics used by illicit procurement networks at each stage of their activities – ordering and purchasing,

shipping, and financing. The authors include methods and warning signs from those case studies in this chapter. Additional tactics and red flags were compiled from information from governments, legal proceedings and indictments, Institute resources, and inter-governmental and non-governmental organizations. Valuable resources included, for example, the FATF warning signs, a Swiss industry outreach pamphlet, German intelligence reports, information from the U.S. Commerce Department's Bureau of Industry and Security (BIS) website, and a list compiled by the non-governmental group, C4ADS, part of a report called Open Arms.[1] A list of references to additional Institute case studies that illustrate various methods and warnings signs is also included in the Annex to Volume 1 of the report.

Rarely are goods adequately described by Harmonized System (HS) or U.S. Export Control Classification Number (ECCN) codes. These numbering systems are too general and often lack specificity to provide confidence by themselves to identify an illicit shipment. They can assist in screening goods, if used carefully.

If a good is being sent to a listed sanctioned entity, but lacks a license or respective export authorization, most parties involved in an export transaction should be able to flag and stop it. The same is true for information that reveals a direct match with a designated entity or their phone numbers and addresses.

The methods and warning signs in this chapter attempt to assist regulators and private sector entities better detect less overt attempts where methods of concealment are frequently employed.

Methods and Warning Signs at the Ordering and Purchasing Level

Illicit procurement networks must conceal the proliferant state customer from law-abiding, vigilant suppliers and their governments. The proliferant state often uses domestic procurement entities or trading companies to search the world for other trading companies or intermediaries to serve as communicators with suppliers, and at times, as claimed end-users. Often, they send or use domestic agents abroad to set up foreign companies. If these entities are located in a non-sanctioned or non-sensitive country, suppliers will often exercise less vigilance over a sale. Government licensing agencies may also be duped into processing export licenses if a controlled good is purportedly destined for a benign or authorized destination and end-user. Increasingly, proliferant states use entities and individuals working from within supplier states to obtain controlled goods. They set up their own small companies there, and since suppliers believe the good will not be exported, they do not need to apply for an export license. In this way, the good can be taken into possession and then surreptitiously exported.

Box 1 is a list of ordering and purchasing methods and tactics used by illicit procurement networks. If applicable, the method is followed by example "red flags" that suppliers and

[1] See: Marcel Angliviel, Benjamin Spevack, and Devin Thorne, *Open Arms - Evaluating Global Exposure to China's Defense-Industrial Base* (Washington, D.C.: C4ADS, 2019), https://www.c4reports.org/open-arms

licensing officials should be aware of. Some red flags are indicators of other illicit trading methods or activities and can be associated with several different methods.

Box 1. Illicit Ordering and Purchasing Methods & Warning Signs

Method 1. Proliferant state obtains goods directly from a supplier located in a state with weak or non-existent trade controls

→ Red Flag: A supplier or one of its subsidiaries in a country with weak export controls is observed having an unusual uptick in sales of sensitive or controlled goods

2. Proliferant state trading companies order dual-use goods for purportedly civilian applications directly from supplier countries, then divert them to the state program; this tactic may involve public tenders bid on by local trading companies; may involve legitimate subsidiaries or distributors of controlled goods located in the proliferant state; may also involve other foreign trading companies or brokers

End-user flags:

→ Inquiries about goods sought for purchase are highly specific, but end-user information is vague or inconsistent with the sought goods, or frequently changes upon questioning

→ The declared end-user is a university or other entity in a proliferant state with known ties to the government

→ The customer sends employees to the supplier for training on the use of a particular good instead of accepting an offer for trainers to come visit on site, or the customer does not want any training, maintenance, or warranty packages that are usually included

→ The end-user given is determined to be a residential address, a small office unrelated to the good's use or one used by other trading companies, a freight forwarding location, or a non-descript warehouse

→ The goods sought by a trading company fall on a "watch list" of items needed by proliferant or sanctioned programs. For a company, this means identifying the potentially sensitive goods it sells

→ Public tenders are observed with requests for those particular goods in proliferant state media

→ Tips are received about a particular proliferant state scheme or supply need from a responsible government

Military customer flags:

→ The customer/trading company is a (foreign) government-listed military supplier or is identified as one that has previously traded or commonly trades in goods with sensitive or military applications

→ The customer appears to host military representatives on site, possibly inspecting production standards

→ The customer appears to have (foreign) defense contractor partnerships

→ The customer appears to have ties to (foreign) defense R&D projects at a university

→ The customer attends or presents at military and defense trade shows, conferences, and forums

→ The customer hosts a (foreign) national laboratory

→ The customer's office is based in a (foreign) defense and security industrial zone

→ The customer appears to provide or receive (foreign) military funds

3. Use of proliferant state trading companies or state-owned or operated entities to send out orders worldwide to potential partner trading companies or brokers; the proliferant state assets and citizens are protected from arrest and prosecution unless they travel abroad

→ The customer obfuscates about business contacts or relationships in the supplier country

→ The trading company has identifiable links to a proliferant state or governmental entities

→ *Individuals hint about business with sanctioned countries in order to elicit potential cooperation with sales offices or agents*

→ *Intelligence shows that the same suspicious inquiry was made to many companies*

4. The proliferant state approaches or recruits trusted persons living abroad to set up trading companies or act as a broker

→ *The customer/trading company has identifiable links to a proliferant state government or governmental entities*

→ *The trading company is small, has no office, no known customers, no website, uses a free e-mail service with no connection to a website domain, has no reviews or social media, or overall has minimal physical or online presence*

→ *End-user flags (See method 2)*

5. Proliferant state traders form enduring relationships with intermediaries in third countries, attempt to establish interpersonal relationships, and promise future, lucrative business, in order to convince them to take greater personal risk or negotiate lower prices (e.g. getting paid late, accepting a lower cut)

→ *Frequent communications and invitations to meet are observed*

→ *Individuals appear to frequently travel to proliferant states*

→ *Individuals make promises of high commissions and large future orders*

→ *While conducting licit business, individuals hint about business with sanctioned countries in order to elicit potential cooperation with sales offices or agents*

6. Use of companies in countries with sound trade controls and no record of illicit trade to obtain goods, and then arranging their illicit re-export or transshipment to the proliferant state via a third party, such as a foreign trading company

→ *End-user flags (see method 2)*

7. Use of a broker: In order to conceal its identity, a company orders from another company in its same country goods from a supplier, located in another country, on behalf of a proliferant state or sanctioned program

→ *End-user flags (see method 2)*

8. Utilization of foreign trading or front companies as intermediaries and communicators on a transaction or as purported end-users/end destinations

→ *The stated end-user is observed to be a trading company with identifiable links to a country of proliferation concern*

→ *An unusual or suspicious amount of communication is noticed between the trading companies and the end-user*

→ *The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry*

→ *The customer is vague about the end-use, does not ask any technical or business questions that are usually asked in similar business interactions, or does not seem to have technical knowledge of the items or knowledge about proper packaging and handling of the items*

→ *End-user flags (see method 2)*

9. Claim made of a legitimate, civilian, foreign entity as a purported end-user, even though the entity did not order the good and has no knowledge of the transaction

→ *The technical specifications or quantity of the good ordered appear inconsistent with the business and size of operation of the stated end-user*

→ *The customer sends employees to the supplier for training on the use of a particular good instead of accepting an offer for trainers to come visit on site, or the customer does not want any training, maintenance, or warranty packages that are usually included*

→ *Outreach to and communications with the claimed end-user demonstrate a lack of knowledge about the order*

10. Goods are purchased as part of a legitimate, civilian procurement order; part of the order is diverted to a proliferant state

→ *The technical specifications or quantity of goods ordered appear inconsistent with the operations and needs of the stated end-user*

→ *Re-exports for part of the order are made and detected in transit*

→ *Post-shipment end-use verification shows that the civilian entity no longer possesses some of the goods*

11. Seeking of less than ideal goods, "just below" in quality or technical specifications of those controlled on direct-use or dual-use control lists, thereby avoiding all but catch-all controls

→ *The customer obfuscates to the supplier about the nature of its business contacts or relationships*

→ *The stated end-use differs significantly from the product's intended use or instructions for its use*

→ *Larger quantities of goods that would fall under catch-all controls are suddenly ordered by multiple trading companies, or by a single trading company, located in known transshipment countries*

→ *A declared end-user is in a country with little ability to use the items*

12. Sending of inquiries about goods to foreign distributors of a primary supplier's goods in hopes they will make a sale

→ *Payment offers are uncommonly favorable for the distributor -- including offers of cash, cash in advance, and high premiums*

→ A distributor in a country with weak export controls is observed having an unusual uptick in sales of sensitive or controlled goods
13. Ordering items in small batches to avoid causing suspicion by the supplier or licensing agency
→ Sales records show small, recurring orders by the same customer or a connected entity, even though there may be economic incentives to buy larger quantities
14. Use of barrage approach: sending out of multiple inquiries for a good to many subsidiaries, daughter companies, or agents of a single company in hopes one will make a sale
→ Several sales managers at a company and its foreign distributors receive the same inquiry from the same or multiple similar sources
15. Use of a corrupt official at a trusted company or its subsidiary, or serving as its agent, to acquire goods and falsify records and documentation, e.g. fabricating a false end-user, exporting the items without a license, falsifying invoices, goods description, and item classification, etc. (so the official can order and export the goods without suspicion)
→ An unusual uptick of sales of sensitive or controlled items by a subsidiary, agent, or distributor is observed, potentially in a country with weak export controls *→ Excessive secrecy regarding a sale is observed, such as use of personal e-mail or phone number instead of company communication channels* *→ An unusual uptick of sales of sensitive or controlled goods by a primary manufacturer is observed* *→ Two sets of books, e.g. phony accounting, failure to apply for licenses, or other falsification efforts are detected*

16. Obtaining goods from within the supplier state so the sale appears to be a domestic sale, then shipping the goods abroad illegally and with false shipping documentation (this bears the risk of arrest for the local intermediary, but avoids the need to supply a false end-user declaration for export licensing purposes)

→ The customer adds packing directions that are not consistent with the declared destination (i.e. sea-worthy packaging for purported inland sale and delivery)

→ The customer sends employees to the supplier for training on the use of a particular good instead of accepting an offer for trainers to come on-site, or the customer does not want any training, maintenance, or warranty packages that are usually included

→ The items are planned for delivery to a warehouse or freight forwarder in the supplier state

→ End-user flags (see method 2)

17. Establishing front companies or illicit operations inside a supplier state for the purpose of gaining access to classified, or export-controlled information, e.g. through contacts at conferences or establishing government contracts

→ A person or entity has ties to a proliferant state government, governmental entity, or sanctioned entity

→ A person or entity lacks legitimate office space, business operations, staff related to his or her stated endeavor, or official communication channels such as a company e-mail address

→ A person conducts overseas trips that seem excessive in number or length of duration

→ Discovery of sensitive documents at a person's home or on his or her computer

→ A person asks suspicious questions at conferences or during meetings, or of other individuals

→ A person or their business entity fails to perform contracted activities or violates rules of contracts

18. Use of aliases to obscure sanctioned or suspicious company names or locations from authorities, bank screening systems, or company compliance officials

→ Addresses, e-mails, phone numbers, or other contact information is identical or nearly identical to a sanctioned entity, or is shared by other trading companies

→ Company agent has ties to a sanctioned entity or proliferant state government

→ Discovery of multiple e-mail accounts for correspondence with legitimate suppliers, where some are only used to communicate with conspirators or a proliferant state

19. Small import/export operations disguise themselves as larger ones, increasing their perceived legitimacy to supplier companies

→ Company address is found to be residential, based on a post office box, is run by one to a few individuals, or the company does not appear to truly exist except for having an office suite address to which mail or parcels are sent

20. Procurement agents or brokers form close relationships with company officials to establish and maintain supplier/client relationships, thereby reducing chances the seller will suspect an illicit scheme or act upon suspicions

→ The agent avoids meeting at his or her company's location, whether locally or abroad

→ The agent or broker has no technical knowledge of the goods sought or no knowledge of the industry or other suppliers located in the supplier country

→ The agent or broker has identifiable ties to a proliferant state government or governmental entity

→ The agent or broker maintains frequent, excessive communication

→ The agent or broker appears to make an effort to please the supplier, e.g. through compliments or favors

21. Network or parts of it are renamed or relocated in the same country once a scheme has been uncovered and entities have been sanctioned
→ New entities involving the same employees or contact information as the sanctioned entity start to appear
22. Agent of a trading company in a country with weak trade controls organizes their own manufacturing capabilities, as described in the case of Cheng operating in China to supply Iran's centrifuge program (Chapters C.1-C.4)
→ A new manufacturer purchases sub-components and specialized machinery, but has no known partners, customers, advertisements, etc., for those goods, and conceals its customers, even from its employees
23. Procurement networks make targeted investments in foreign companies to obtain access and control over the production of sensitive goods and technology
→ Seemingly unrelated investments, e.g. in foreign manufacturing companies, prove to have a connection to proliferant state efforts

As proliferant states' covert or sanctioned programs evolve, they may set up their own transnational supply chains, and most threateningly, these may start to supply other pariah states. The A.Q. Khan network out of Pakistan's nuclear program was the first semi-autonomous illicit trade network. In this case, the network had "gone rogue" from the proliferant state and started offering turn-key nuclear weapons programs to other states without the Pakistani government's full awareness. North Korea represents a state that has provided nuclear commodities and capabilities to others, such as a nuclear reactor to Syria, likely using its illicit procurement networks. The Khan network also put in place off-shore manufacturing capabilities in Malaysia, Switzerland, Turkey, South Africa, and elsewhere to supply Pakistan's and other countries' needs.

Box 1.1. Proliferant State as Supplier Schemes

24. Rogue or semi-autonomous illicit trade networks grow out of state-run illicit procurement efforts, even offering commodities or capabilities to other states (A.Q. Khan network out of Pakistan selling to Libya, Iraq, Iran, others alleged)

→ *General warning signs of illicit trade apply*

→ *Visits are observed by senior WMD or missile officials from a country of proliferation concern to a pariah state, including in violation of international sanctions, e.g. involving persons under a UN travel ban*

25. Proliferant states outfit others using their domestic capabilities and established procurement networks (e.g. North Korea selling to and outfitting Syria)

→ *Facilities, missiles, or other weapons display similarities to known ones in other pariah states*

→ *Visits are observed by senior WMD or missile officials from a country of proliferation concern to a pariah state, including in violation of international sanctions*

→ *Anomalies in procurements by a pariah state are observed*

→ *Similarities or parallels in procurements between two or more countries of proliferation concern are observed*

26. Proliferant state operates manufacturing sites in foreign countries that supply key components

→ *Excessive secrecy or lack of known customers are observed at sites or facilities*

→ *Nationals from a country of proliferation concern appear to be involved in supervising roles, including training and management*

→ *Former nuclear, missile, or other weapons experts are observed at a facility*

→ *Known, past or current strategic commodity traffickers are observed at a facility*

Methods and Warning Signs at the Financing Level

Proliferant states and their illicit procurement networks must finance and submit payments for strategic commodities, often by disguising the origin of financial transactions. The most sophisticated proliferation financing schemes route bank transactions through several countries before the funds finally reach the supplier state and its bank account. Countries that carefully enforce UN sanctions and domestic laws against transactions with countries of proliferation concern require banks to bear some onus in preventing proliferation financing. Banks must report transactions over a certain amount, not process transactions and freeze those associated with sanctioned countries, entities, or individuals, and report transactions attempted by such parties. Because illicit networks can conceal names of individuals and entities, and rarely list controlled goods as part of a financial transaction, it is particularly difficult for banks to detect proliferation financing schemes. Often only repeated, suspicious transactions or indications of the involvement of banned parties, entities, or countries will tip off financial institution compliance personnel to the possibility of illicit transactions. Moreover, illicit networks use increasingly modern methods in the realms of cyber-hacking, virtual thefts from banks, and thefts of cryptocurrency.

Box 2 is a list of proliferation financing methods and warning signs that can be used by financial institutions, government regulators, and companies to help identify, halt, and investigate potentially illicit payments. They were gathered for this report from strategic commodity trafficking cases, proliferation financing reports, UN Panel of Experts reports on the implementation of Iran and North Korea Security Council resolutions, FATF's indicator lists, and U.S. and foreign government guidance.[2] Some of the indicators and methods could define as both.

Box 2. Proliferation Finance Methods & Warning Signs

27. Payments for controlled or proliferation-sensitive goods and services are not described in financial transaction paperwork; if required, the stated reason for payment is false or mischaracterized

→ *A payment appears too high for described goods and services*

→ *The origin of the payment is a state that transacts frequently with sanctioned countries*

[2] Additional, useful case studies have been prepared by Jonathan Brewer, *Study of Typologies of Financing of WMD Proliferation* (London: Project Alpha, King's College, October 13, 2017), https://projectalpha.eu/wp-content/uploads/sites/21/2018/05/FoP-13-October-2017-Final.pdf

→ *Aliases and phony good descriptions are used*

→ *Description of goods is nonspecific, innocuous, or misleading*

28. Intermediaries in third-party countries, such as trading companies, order items and route proliferant state payments to supplier country banks using local banks, other country transaction hubs, or personal accounts

→ *Transaction involves possible front or shell companies*

→ *Transaction involves intermediary that appears to have little on-hand capital but makes frequent financial transactions*

→ *Multiple different trading companies or front businesses are operated by the same individual(s) and are registered to the same location*

→ *Shared addresses, e-mail addresses, and employees are observed as involved in financial transactions relating to suspiciously different types of business or procurements*

→ *Involvement is observed of a small trading, brokering, or front company, often carrying out business inconsistent with their normal business*

→ *Address of an entity appears to be residential or unrelated to its claimed line of business*

→ *Staff lists and addresses provided by a company are inaccurate or fake*

→ *A company has no website, no social media, no business directory presence, or an overall minimal online presence*

→ *A company has identifiable connections to pariah or sanctioned countries*

→ *Involvement is observed of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business*

→ *Financial transactions are observed being carried out by an entity whose ownership has gradually transferred to being foreign-dominated*

→ Entities or individuals are involved in financial transactions but have little actual physical presence or business operations in the host state

→ A transaction demonstrates links between representatives of companies exchanging goods, e.g. same owners or management

→ Directors of an entity or company suddenly or frequently change

→ Banking or trading activity does not match the business or account profile, or end-user information included in a transaction does not match the business' profile

→ "Cycling" is observed, where there is involvement of certain bank accounts and front companies in financial transactions, after which a period of dormancy follows

→ Patterns of wire transfer activity appears unusual or has no apparent purpose

→ A customer is vague/incomplete on information they provide, and resistant to providing additional information when queried

→ A new bank customer requests a rushed letter of credit transaction while awaiting approval of new account

→ Wire instructions or payment from or due to parties who are not identified on the original letter of credit or other documentation are observed

→ Multiple, successive transfers are made from the same sender or to the same beneficiary or connected accounts, within a short period of time, even while uneconomical due to recurring transfer fees (done to avoid bank reporting requirements that would invite scrutiny, or to make partial or upfront payments for items)

→ Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak trade control laws or weak enforcement of trade control laws

→ Trade finance transaction involves shipment route (if identifiable) through country with weak trade control laws or weak enforcement of trade control laws

→ Financial transactions are made involving goods that seem unrelated to the nature of the company's stated business

→ *Trade financing documents show a freight forwarding firm listed as the product's final destination rather than a legitimate end-user*

29. Proliferant state makes use of domestic or government-owned airline or shipping assets to move cash, gold, or other valuable liquid assets

→ *Transaction involves person or entity in country of proliferation concern*

→ *Open source or intelligence data tracks suspicious activity and use of these assets*

30. Transactions made via multiple banks that obscure the country of origin of payments

→ *Circuitous routes are used for financial transactions*

→ *Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated)*

→ *A transaction made for goods is placed by firms or persons from countries not located in the country of the stated end-user*

31. Removal or omission from financial entity paperwork of sanctioned country addresses, names, and entities to obscure origin of transaction

→ *A customer or counter-party or its address or phone number is similar to parties found on publicly available lists of "denied persons" or has a history of trade control violations*

→ *Individuals involved in a company's ownership are observed to also hold ownership or share physical addresses with sanctioned, sanctions-busting, or high-risk entities*

→ *Individuals are unwilling to provide or raise difficulties in providing additional information about their bona fides or activities*

32. Establishment of foreign bank branches or correspondent banking relationships by a proliferant state or its illicit agents and companies, in order to facilitate illicit transactions; often occurs in jurisdictions or countries with weak or lax financial controls (including offshore banking havens)
→ *Transaction involves a bank or account with identifiable ties to a country of proliferation concern* → *Ownership or significant control of shares are identified or observed as linked to a sanctioned or pariah country*
33. Use of intelligence agencies to carry out illicit financial activity, including cyber-hacking
→ *Computers, servers, or logins have been compromised and signs point to state-level efforts of a country of proliferation concern*
34. Use of nationals abroad to withdraw or transfer funds located in foreign banks
→ *Involvement in a transaction is observed of person(s) who relate to a country of proliferation concern*
35. Use of bordering or regional country banks to facilitate illicit financial activities, including involvement of key countries or territories in transactions
→ *Entities or individuals are involved in high-risk banking or correspondent banking relationships with entities previously involved in financial sanctions evasion; some border sanctioned states*
36. Use of proliferant state-owned entities to transfer original payments for illicitly acquired goods, e.g. national or central banks or state universities
→ *Involvement in a sensitive transaction by a university in a country of proliferation concern*

→ *Involvement in a sensitive transaction by a national/central bank of a country of proliferation concern*
37. Intermediaries establish own bank accounts in proliferant states to receive payment for goods, including commission
→ *Individual makes frequent travels to a proliferant state while operating a business in a foreign country*
38. Use of personal bank accounts to facilitate movement of funds
→ *See method 28*
39. Use of currency exchanges to convert money from sanctioned country denominations to desired currency
→ *See method 28*
40. Use of revenue streams from benign or humanitarian trade to finance proliferation-relevant activities **41. Purchase of banned goods (e.g. endangered animal parts) from a third-party country and smuggling them to another country, where they are sold, to move the hard currency back to the proliferant state or use it to purchase items in that state** **42. Establishment of revenue streams that fund proliferation activities using foreign business partnerships, military training services, and other commodity trading activities (e.g. coal, petroleum)** **43. Use of precious metals or other material assets to finance illicit commodity purchases** **44. Payment via bulk cash, often moved transnationally**

→ Sanctioned entities are involved in and appear to be the beneficiaries of business activities *→ Foreign officials or agents return from visits to proliferant states with large amounts of cash (e.g. discovery of undeclared cash at customs)*
45. Simultaneous ATM cash withdrawals are made from various countries and banks in order to remove large amounts of cash from the host countr(ies) and avoid electronic banking transfers
→ Bank records show multiple, apparently coordinated, ATM withdrawals
46. Use of proliferant state officials to physically move money using diplomatic pouch and/or pay for goods via local embassies
→ Business-like transactions or payment for industrial goods originate from embassies
47. Use of trading companies and couriers in third-party countries to deliver funds to complicit or non-complicit exchange houses and receive desired currency for transfer back to proliferant state
→ See method 28
48. Use of professional services, such as accountants or law firms, or non-profit groups, as fronts for illicit finance
→ See method 28
49. Use of virtual currencies (cryptocurrencies or "convertible virtual currencies (CVCs)") to finance illicit strategic commodity purchases, such as Bitcoin
→ Payments tied to the purchase of industrial goods are made in cryptocurrency

50. Counterfeiting of currency for proliferation-related activities
→ *Proliferant state has been observed procuring equipment suitable for the production of counterfeit bank notes*
51. Ledger transactions (known as "book-to-book"), in which companies or banks write off funds for proliferation finance based on money received for other, legitimate or non-legitimate transactions
→ *Phony or problematic accounting methods are observed by authorities*
52. Use of aliases, falsified company names, obscured sales records, and obscured country of origin to set up bank accounts in order to bypass financial institution screening tools
→ *See method 28*
53. Proliferant state agents obtain foreign dual nationality/citizenship/passport to enable illicit financial transactions in foreign countries
→ *Customer has identifiable ties to a proliferant state government*
54. Use of cyber-attacks by state or state-backed entities in order to steal funds from financial institutions, including cryptocurrency exchanges
→ *Cyber-attacks are linked to agents working in or for proliferant states*
55. Use of barter arrangements for payment
→ *Intelligence or informant information indicates trade of controlled or sensitive goods by one government to a proliferant state in return for other goods or services*

56. Establishment of state-run cryptocurrency exchanges intended to help circumvent financial controls and sanctions

→ *Intelligence or other information indicates the existence of such an exchange*

Methods and Warning Signs at the Shipping Level

Once successfully ordered and paid for, the next key question for an illicit procurement network is how to move commodities from the supplier state to the proliferant state without being detected. The network must bypass scrutiny by customs and shipping companies which attempt to detect the unlawful export of controlled commodities. This results in the most sophisticated networks using several layers of deception to conceal the true contents of packages. If an illicit network operative is working from within a supplier state, once they have received the commodity at the purported domestic end-user location, they can change the packaging and shipping labels to hide the supplier, undervalue the contents so that lower values may not have to be reported to export authorities, arrange for new shipping labels at the transshipment point, and remove invoices characterizing the nature of the goods in case the package is opened by shippers or customs authorities. If such a package is stopped at customs, only trained customs officials would be able to identify a controlled item and flag it for greater scrutiny. Similar conditions exist for goods that receive export licenses under false pretenses. If a licensed good is stopped for extra scrutiny, it is even less likely that customs or shipping authorities would request more information about its intended recipient, either from licensing authorities or the supplier. Stopping an illicit procurement at the shipping level is thus much more difficult and leaves fewer observable indicators of illicit activity than the ordering process. Box 3 is a list of common shipping methods used by illicit procurement networks and warning signs for those seeking to thwart them.

Box 3. Illicit Shipping Methods & Warning Signs

57. Use of trading companies abroad, even multiple trading companies located in different countries, to transship goods to a proliferant state, obscuring the actual end-user

Recipient flags:

→ Shipment of sensitive goods goes to a trading company or possible front company in state with poor strategic trade controls

→ Address of a recipient is residential, a small office suite, a post office box, or is otherwise unrelated to the purchase

→ Recipient on transport documentation is inconsistent with information on the invoice, customs declaration, or other documentation

→ Recipient has identifiable ties to a proliferant state's government or appears unrelated to the described goods

→ Recipient often orders or receives military goods

→ Address of recipient is based in a defense and security industrial zone

58. Transshipment or re-export of goods using circuitous routes and/or multiple countries to hide the actual end-user

→ Packaging or packaging directions do not appear to make sense given the transportation route, e.g. sea-worthy packaging for in-land transport

→ During transit, the mail-to end recipient upon exit from a country is different from that stated upon entry

→ A transportation route for a parcel does not seem to make sense geographically or economically

59. Transshipment of goods through a Free Trade Zone or similar customs-exempt zone

→ Sensitive, expensive, or highly-specialized goods are destined for storage in a Free Trade Zone, customs-bonded warehouse, or similar

60. Goods are sent to a freight forwarder in a foreign country, especially one that is not a national security priority; from this location, the goods are illegally shipped onwards

→ *Address of recipient is possibly a freight forwarder or logistics company*

61. Upon *shipment,* customs, shipping, and product labels or documents are altered to have phony product descriptions, undervalued contents, or hide the goods' nature

→ *A shipping agent is instructed to remove documents such as invoices, labels, stickers, handbooks, or instruction manuals*

→ *A shipping agent is instructed to use a vague or falsified goods description*

→ *The declared value of the shipment appears too low*

62. Upon *transshipment*, customs, shipping, and product labels or documents are altered to have phony product descriptions, undervalued contents, or hide the goods' nature

→ *Recipient on transport documentation is different from invoice, customs declaration, or other documents*

→ *Address of recipient is residential, a small office suite, a post office box, possibly another freight forwarder or logistics company, or is otherwise unrelated to the item description*

63. Use of proliferant state-owned shipping assets or airlines to move commodities

→ *Observed use of proliferant state entities to transport goods*

→ *Unconventional activities observed, such as off-loading of goods and transferring them from one plane or ship to another*

→ *Ship-to-ship transfers of commodities, occurring in international waters, and often at night*

→ *Turning off of ship AIS or plane transponders or GPS signaling to obscure location*

(See also Box 3.1 below)

64. Use of proliferant state entities, including financial institutions or embassies, as purported shipping end destinations

→ *Proliferant state entity is listed as the consignee, or is listed as the final consignee for transshipment*

65. Upon inspection, dual-use items are observed and the goods are not subject to trade controls, but are similar or close to the capability of goods found on export control lists

→ *Recipient has identifiable ties to a proliferant state's government or a governmental entity*

→ *Recipient appears unrelated to the described goods*

→ *Goods have similar characteristics, including type and number, as items known to be for a sanctioned, secret, or sensitive weapons program*

→ *Goods are observed moving via a personal vehicle or truck that is moving other types of goods (cargo appears smuggled among other goods)*

66. End-user of requested strategic goods is listed as located inside the supplier nation and is then exported illegally to proliferant state to avoid obtaining an export license

→ *Address of the "domestic" end-user/recipient is residential, a small office suite, a post office box, or a freight forwarder or logistics company, or is otherwise unrelated to the item description*

→ *Packaging or packaging directions do not appear to make sense given the transportation route, e.g. sea-worthy packaging for domestic, in-land transport*

→ Shipping agent/freight forwarder is instructed to or acts to falsify labels, or remove labels, invoices, or other documentation, before an export overseas
67. Use of responsible supplier nations as transshipment points by companies or entities cooperating with proliferant states, due to reduced scrutiny of the initial export
→ See method 66
68. Shipments of illicit goods are arranged by corrupt or rogue sales agents of the supplier company
→ Supplier has unusual requests, such as to remove labels, invoices, or other documentation before shipment *→ Un-official communication routes are used by a company official to place shipping and packing orders* *→ Payments to a shipping agent are made in cash or from personal accounts instead of company accounts*
69. Illicit procurement agents deceive supplier sales agents into believing sanctions are no longer applicable/non-existent in order to approve shipments
→ Screening software used by a shipping agent finds that an address, e-mail, phone number, or other contact information is identical or nearly identical to that of a sanctioned entity
70. Request for strategic goods shipments from companies that do not have adequate trade control policies or a compliance department
→ A shipping agent receives unusual instructions from or otherwise witnesses poor knowledge of trade controls by its customer

71. Fraudulent use of legitimate business names and credentials to illicitly obtain export licenses and strategic goods
→ *Recipient flags (see method 57)* → *Use of non-company e-mail platforms, such as Gmail or Yahoo*
72. Goods are moved via a person, their luggage, or a vehicle that is moving other types of goods (cargo is smuggled)
→ *Industrial-appearing or incongruous-looking goods move with a person, in personal luggage, or in a personal vehicle* → *Cargo is observed in a vehicle that is not congruous with the majority of the other cargo* → *Sensitive-appearing goods, manuals, etc. are not declared or are observed as part of cargo*
73. Rogue agents at a supplier state company knowingly and willingly incorporate controlled goods into shipments of non-controlled goods, to better conceal their nature
→ *Use of non-official communication, such as personal e-mail addresses or private mobile numbers, by company officials to arrange shipping and packaging* → *Incorrect, fraudulent, or phony accounting books are observed or discovered by company officials or compliance personnel*
74. Use of falsified export documents, purchase requests, shipping requests, invoices, and end-user documentation to illicitly export goods
→ *Documents appear altered, are missing official company letterheads, or contain contradictory or inconsistent information*

75. Issuance of a bill of lading with a false recipient for customs clearance, but subsequent re-issuance of the same bill of lading with an edited end-recipient for the transport provider

→ *Recipient on documentation carried by the transport provider does not match the recipient in the (electronic) customs record*

76. Shipment of small quantities of sensitive or controlled goods in several small packages to avoid customs scrutiny

→ *Records show that several packages from the same sender or a connected party are sent to an identical or almost identical recipient on the same day or within a short period of time*

→ *A parcel is sent to an individual at an address of a known sanctioned entity, rather than being addressed to the sanctioned entity (so the shipment appears related to personal uses)*

Box 3.1. Maritime and Air Illicit Shipping Methods & Warning Signs

79. Changing of names, flags, registrations, and other identifiers of cargo vessels, planes, or ships involved in sanctions-violating activity to "camouflage" their origin and purpose

→ *Screening a vessel or plane's data history shows frequent changes and alterations*

80. Ship-to-ship or STS transfers of illicit goods are made between (potentially disguised) cargo ships in international waters for delivery to proliferant state

→ *One or several vessels have altered their name, flag, IMO number, and other physical identifiers*

→ *An STS transfer occurs at night*

→ One or both vessels switch off their AIS

→ Commercial or governmental overhead imagery or ground photographs reveal suspicious STS activities

→ Numerous small vessels appear to approach one larger vessel for an STS over the course of several hours and depart to the same port

→ Ships receiving goods via STS often dock at a frequent recipient port for banned commodities

81. Broadcasting of a false identity via the vessel's AIS

→ The vessel's broadcasted name or IMO number does not match the name on the vessel's hull or other physical identifiers of the ship

82. Disabling or manipulating a vessel or airplane's transponder, radar, or GPS to hide its movements

→ Screening a vessel or plane's record reveals frequent periods of silence, especially when operating near proliferant states

83. "Laundering" of commodities, or selling goods originating in a sanctioned country as though they are from another, non-sanctioned country

→ Vessels or airplanes are observed in satellite imagery or other photographic evidence carrying commodities from a proliferant state, docking or landing at/in a non-sanctioned country, and off-loading or mixing commodities, which are then delivered to other countries

→ An AIS-broadcasted draft or plane transponder location has changed after a period of "silence" or is otherwise inconsistent with a vessel or airplane's alleged pick-up and drop-off route

84. Registration of a vessel or plane in a different country or in a so-called "flag of convenience" state to avoid scrutiny or oversight
→ The vessel or airplane's owner and operator are not based in the country of registry *→ The vessel's flag or the airplane's country of registration is changed frequently*
85. Obfuscation of a ship's voyage by lingering outside a port or adding unnecessary stops and detours
→ Port data and AIS data appear inconsistent with common shipping routes and practices
86. Use of small vessels or planes without the physical identifiers carried by larger ships or planes, and less powerful AIS signaling, for STS transfers
→ Multiple STS are observed to be performed sequentially with small vessels, instead of with one large vessel; these small vessels are observed off-loading the commodities at the same port *→ Small planes are observed exchanging goods and then returning to or heading to sensitive countries*

Chapter 14. Policy Implications and Recommendations

A major focus of this report is to better understand the strategies and tactics of those states and networks undertaking illicit procurement for nuclear, missile, and conventional military programs. A key observation is that a wide variety and quantity of goods are needed by those undertaking illicit trade, far beyond what is commonly believed. Moreover, while traffickers and their accomplices are adept at defeating and otherwise bypassing trade controls and sanctions, governments have proven remarkably skilled at detecting and stopping these efforts. Although completely stopping such illicit activity will never be a realistic goal, governments have managed to make the illegal acquisition of key sensitive commodities far more difficult and expensive, causing shortfalls and delays in augmenting sanctioned and otherwise destabilizing nuclear, missile, and conventional military programs.

However, those committed to illicit trade, in particular Iran and North Korea, among others, remain determined to acquire needed goods and seek to exploit weaknesses and loopholes in the existing controls and sanctions. As a result, improving countermeasures must remain a priority. The ultimate aim of U.S. and partner country policies should be to continue bolstering their defenses and better hone their offenses in order to create an improved counter-proliferation system as a whole. This report and its recommendations are viewed as a way to contribute to that effort.

The case studies in this report also lead to a series of recommendations that are presented in this chapter, which the United States and likeminded countries can use to more effectively detect and prevent illicit procurement today and in the future. This chapter is intended to draw out several areas where fixing or augmenting policy would be highly beneficial in terms of high order value and impact, with a focus on U.S. actions. A broader set of recommendations for improving national strategic trade controls and international sanctions can be found in the 2017 edition of the *Peddling Peril Index*.[1]

Discussed here are a dozen recommendations that would complement and strengthen U.S. and partner government efforts to better perform in a range of counter-proliferation areas, including timely detection of illicit trade, export licensing, outreach to the private sector, improved enforcement internationally, detection of proliferation financing, and improved controls over shipping. The recommendations would assist the enactment and tightening of sanctions against countries and their illicit weapons programs. Private sector actors also have a stake in understanding how they may contribute to greater national counter-proliferation missions and prevent their businesses from being exploited by illicit networks.

[1] David Albright, Sarah Burkhard, Allison Lach, and Andrea Stricker, *The Peddling Peril Index 2017, Institute for Science and International Security,* January 31, 2018, http://isis-online.org/ppi/detail/peddling-peril-index-ppi-2017/

Better Detecting Illicit Trade

A first priority of policy goals concerns counter-proliferation methods to more effectively detect illicit trade. These recommendations can be divided into two broad areas—corporate responsibility, and investigations by intelligence and enforcement entities.

1) The private sector should better understand the methods and warning signs of illicit networks and undertake stronger due diligence efforts

One lesson from this report is that it is possible for suppliers, shippers, and financial institutions to detect illicit or questionable trade. But many companies do not make stopping illicit trade a priority. Moreover, a few company officials are corrupt and willing to participate in illicit schemes for financial gain.

To be responsible, all companies need to institute internal compliance systems (ICPs), proportional to their size and the potential dual-use nature of their products. Each company should undertake to know and identify their customers and establish company-wide policies that include maintaining strong relationships and communication with, and oversight of, foreign subsidiaries and agents. They should apply the same rigid scrutiny to sales, shipments, or financial transactions by overseas affiliates that they would for domestic transactions, and regularly provide training to foreign company officials on due diligence and legal requirements.

Too often today, companies overly rely on software that matches buyers with listed or suspicious entities or individuals. Although this approach is one aspect of a successful ICP, compliance personnel and the human brain are needed to identify illicit schemes.

A special concern involves trading companies. They are a critical and typically legitimate aspect of conducting business; however, they also pose one of the more challenging problems of detecting illicit trade. Suppliers of potentially sensitive goods need to insist on knowing the actual end-user of goods before making a sale. Although many trading companies worry about "end-runs" by suppliers, who then make a direct contact to the buyer and eliminate the trading company in the process, the risk of not knowing the actual end-user is too great to allow this trading company loophole to exist in corporate compliance systems. Corporate policy should be that if a trading company is not willing to provide the end-user, or appears to withhold information, the supplier should not be willing to make a sale.

However, corporate actions are not enough. They cannot always stop, for example, dedicated criminal activity within a company aiming at undermining corporate controls, such as insider schemes run by rogue agents. Suppliers are also sometimes simply unable to detect the schemes aimed at illicitly obtaining their goods.

2) Intelligence and enforcement communities need to maintain a high priority of detecting illicit trade in strategic commodities

The case studies in this report highlight the key role intelligence and enforcement entities play in acquiring information about illicit procurements. Acquiring this information requires not only devoting resources and expertise to understanding domestic company supply potential and understanding the strategic commodity trafficking networks and agents targeting domestic suppliers, but also understanding the situation abroad. Much information cannot be learned through the export licensing process, since those individuals and trading companies pursuing illicit trade are unlikely to seek a license for their illegal exports. The U.S. intelligence community and enforcement entities, including the Federal Bureau of Investigation (FBI), Department of Homeland Security's Homeland Security Investigations (HSI), and the Commerce Department's Office of Export Enforcement, are world leaders in acquiring information about foreign illicit networks. Many allies, particularly Britain and Germany, also emphasize acquiring this information. However, most other countries rarely prioritize gaining such information. In particular, China has not done so.

The United States should use diplomacy and its outreach programs to encourage key countries to improve their own domestic intelligence and investigation capabilities to better know their countries' supply potential and the illicit networks active there. This also requires coordination with the country's foreign intelligence entities, which likewise need to prioritize detecting illicit trade. The United States should recruit Britain and Germany in this outreach effort.

Toward this goal, the United States should develop a priority list of nations, based on their supply and transshipment potential and relatively poor engagement level of their domestic intelligence and enforcement agencies, as initial targets of this outreach. China should be on this list.

3) U.S. government should continue to better harness and assess data on illicit trade

In detecting illicit trade, a recurring problem is picking out the relatively small number of illicit transactions among the hundreds of millions of legal ones occurring each year. Vast amounts of trade, shipping, and financial data exist. The U.S. government has developed and deployed "big data" analytical tools to assess these data both within and outside the intelligence community. An example of a non-intelligence system is the Border Enforcement Analytics System (BEAP) created under HSI of the Department of Homeland Security, initially at Northeastern University, and now run at DHS on an operational basis. This system allows far deeper probing of illicit trade network-related export data. It applies open-source technology against several large-scale export and import data sets accessed through its customs authorities. Under U.S. law, all exporters shipping goods valued at over $2,500 must declare their export and provide critical information about the goods, recipients, and shippers. Likewise, importers are required to file their declarations with the government. BEAP, and any similar successors or programs, are examples of U.S. government systems that have combined electronic customs data and the advanced analytic tools to interrogate this massive data set for

relevant counter-proliferation violations in real-time, making the results accessible to U.S. border enforcement and counter-proliferation organizations.

In addition, to be effective, these tools require careful searches of the data and further analysis of the results. Toward that end, there is a need for subject matter experts (SMEs) to be part of the process of operating these systems. Moreover, the tips garnered through these systems require follow-up by enforcement agencies. More resources are needed for SMEs to make these systems more effective as enforcement tools and the enforcement agencies need to prioritize the follow-up.

One promising new piece of legislation, the "Supporters of Corporate Transparency Act," was passed by the U.S. House of Representatives in October 2019.[2] It would also assist with federal data gathering and detection of illicit trade by creating a legal requirement for U.S. companies to disclose to the Treasury Department their beneficial owners at the time of their formation. The bill is designed to prevent the operation of shell companies and stem money laundering. The continuing development and improvement of such data systems is critical. Such capabilities should also be created for shipping and financing, if they are not already underway.

4) U.S. government should more frequently exploit and comprehensively assess illicit trade evidence from federal or other prosecutions on an unclassified, albeit confidential, basis

Evidence gathered in the federal prosecutions of key illicit networks provides important insight into strategic commodity trafficking. Often, the collected information far exceeds that used in a prosecution. The information in these cases frequently points out other active schemes tangential to the target network or actors, new threats and loopholes to close, and methods for better thwarting illicit trade. New prosecutions and other counter-proliferation responses can be built from important case information.

There should be a directed U.S. effort to produce reports on important cases and evidence, on an unclassified but confidential basis, and to distribute them to the U.S. interagency system. This effort should be managed by the responsible federal prosecutor in consultation with the enforcement agencies that developed the evidence. Funds to support this work should be drawn from enforcement agencies and the State, Commerce, or Defense Departments.

[2] Jacob Rund, "House Passes Beneficial Ownership Disclosure Bill," *Bloomberg Law,* October 22, 2019, https://news.bloomberglaw.com/corporate-law/house-to-vote-on-beneficial-ownership-disclosure-bill

Bolstered U.S. Government/Industry Cooperation to Thwart Illicit Trade

5) U.S. government should share with responsible companies the latest illicit procurement schemes and tips through enhanced, voluntary cooperation with the private sector

Companies with robust, effective internal compliance programs provide one of the greatest chances for preventing proliferant or sanctioned states from obtaining the goods they seek. They represent an invaluable front line of defense against illicit trade.

Robust government/industry cooperation should involve collecting and sharing sector-specific data on trade, shipping, and financial transactions, and voluntary, two-way information sharing, on the latest illicit procurement schemes. Under such a system of government/industry cooperation, suppliers and shippers would routinely provide the U.S. government with needed illicit trade information. In the case of suppliers, they would share suspicious requests for equipment that could originate in a sanctioned or sensitive weapons program, or from actors about which the supplier has suspicions. This information typically exists in the form of requests for price quotes, or inquiries, and other communications with a potential buyer involving goods specifications, trading companies, transit points, financing, end-uses, or end-user information. Shipping companies also gather key information that raises red flags or concerns while preparing to transit or ship goods. Instead of private sector actors keeping this information to themselves, it would be delivered to the U.S. government, whether or not the supplier or shipper ultimately identified a suspicious actor behind the attempt and decided not to make the sale or shipment.

In return, the government recipient, acting together but with the assistance of their home agencies, would inform companies about the latest illicit procurement and shipping schemes and known equipment needs of proliferant states or other suspect entities, in the form of actionable warning letters delivered on a timely basis.[3] To do so, the governmental entity would need the authority to selectively, or in single instances, secure declassification of warning information that could help a company avoid making a sale or shipment to a proliferant state. The company would be required to treat this information as confidential. One possibility is requiring key company compliance officials to obtain public trust clearances, or another form of vetting that allows access to unclassified information, to ensure the government is providing information to trusted sources.

For the U.S. government, its capabilities would be enhanced in identifying current and emerging methods in illicit trade, finding early detection opportunities, successfully disrupting illicit networks, making interdictions, and gaining strategic intelligence on covert proliferation efforts. Companies would lower their risk of inadvertent exports, and they could demonstrate their good citizenship.

[3] To be effective, the warning letters should include the names of entities and individuals seeking the goods and the type of goods sought, with as precise information as possible about the specific model.

It should be noted that companies would require an unclassified but confidential method to provide information to the government, preferably a designated entity that is not explicitly part of the U.S. intelligence or enforcement communities. They would also require aspects in such a system that provide confidence that they would receive mitigated penalties if cases of wrongdoing were uncovered, as is commonly done when companies admit to the government that they have made inadvertent, illicit exports, in the form of voluntary self-disclosures or their equivalent. The risk run by company compliance and legal departments is that without a reasonably safe harbor for sharing information, they fear they run the risk of provoking unwanted investigations into past inadvertent, illicit sales or shipments, and would advise management against participation in a voluntary program. Of course, participation in a two-way information exchange would not preclude companies from facing civil or criminal penalties, but it should clearly reduce downsides of participating. As a result of participation, companies should feel more confident that the sales and shipments they make will not lead to public embarrassment, reputational damage, criminal charges, or fines. They should also feel they gain by not having to wait on the government to update formal guidance and sanctions lists with up-to-date intelligence on entities, individuals, or schemes of concern.

A robust system of government/industry cooperation on illicit procurement information exists in Britain and Germany, where officials have been willing to share lessons and frameworks. In the United States, this type of system has been explored, but has regularly run into classification obstacles for the government and liability issues for companies. As such, this type of information sharing has only been carried out informally by officials at key agencies, or generally, in the form of outreach to companies through enforcement agencies. Although these programs are valuable and should continue, they are not the same as a regularized system that receives and provides timely warning information. Despite the obstacles to this type of cooperation in the United States, it is worth implementing.

More Universal and Effective Enforcement

The United States has developed an effective enforcement system against illicit trade in a range of sensitive civil and military goods. Throughout the United States, federal prosecutors, supported by the FBI, DHS's Homeland Security Investigations, and Commerce's Office of Export Enforcement, and other federal and state entities, routinely prosecute violators of U.S. export control laws. These enforcement actions deserve support. However, other countries' enforcement of violations of strategic trade control laws and their implementation of sanctions lags dangerously.

6) The United States should expand its outreach and diplomatic efforts to convince many more countries to prioritize the criminal enforcement of strategic trade controls and sanctions

A U.S. goal should be to seek more countries making it a national priority to prosecute crimes of illicit nuclear, missile, WMD, and military goods trafficking and establish trained units within

investigatory agencies to further this purpose. Because of the technical complexity of many strategic export cases, the United States should press countries to:

a) Cooperate with other nations on prosecuting strategic commodity traffickers.
b) Set up procedures to exchange sensitive law enforcement information on illicit trade attempts, within the country's agencies and externally with foreign countries.
c) Extend mandatory minimum sentencing guidelines to make violations of export control requirements, especially those related to WMD, worthy of longer sentences. This is especially important in single markets, such as the European Single Market, so that exporters intending to violate export controls cannot knowingly violate laws in countries with the mildest penalties. Sentences of more than five years in prison and fines appear to better deter violators.
d) Establish a specialized national court responsible for national security cases rather than having local courts take on cases.

Assessments of the Undermining of Control Lists

7) U.S. government should better prevent illicit procurement of subcomponents targeted by illicit trade networks and proliferant states, and subject them to licensing and add them to control lists, if necessary

A growing problem underscored by this report is the tendency of proliferant states to turn to illicit procurement of subcomponents of controlled goods for use in a domestic industry to finish the manufacturing of a desired good. Iran is doing this, for example, in the case of pressure transducers, vacuum valves, and other items, and is attempting to further indigenize its nuclear equipment production over time. The U.S. Homeland Security, Commerce, Defense, Energy, and State Departments, the U.S. intelligence community, and national nuclear laboratories and other research entities, need to work closely to identify and head off emerging threats of countries seeking subcomponents for illicit purchase.

The U.S. government should also list under licensing requirements and add to control lists these subcomponents if nuclear, missile, or military programs appear to be seeking them. This will necessarily entail intelligence information vital to understanding how proliferant states are reverse-engineering key equipment and identifying remaining illicit procurement needs of countries. With regard to this approach by illicit networks, the United States should work to improve understanding internationally among governments and companies about the seeking of these goods by proliferant states. It should assist partner countries' access to technical expertise or "reachback" when suspect goods are detected or seized and their officials require timely analysis as to the goods' purpose and potential misuse.

Countering Proliferation Financing

Countering proliferation financing remains a difficult area in which to make progress, but even as technology is exploited by illicit networks to route payments for goods, it can also be harnessed toward better detection of data that shows illicit activity. Counter-proliferation financing efforts must continue to be bolstered internationally. This requires leadership by the United States, as the global financial center of the world economy. Intelligence sharing is necessary, as well as instituting stronger regulations on virtual currencies. Defenses against cyber-hacking and electronic thefts of funds also need to be improved as states increasingly turn to more virtual methods of funding proliferation. Three specific recommendations seem particularly timely:

8) Governments need to better share intelligence to identify non-traditional illicit payment schemes

Governments are hindered in detecting those transactions that are entirely opaque to the traditional financial sector, for example, barter or book-to-book transactions, where one good or service is traded for another, or done via bulk cash payments or currency conversion schemes. To overcome these challenges, governments need to better deploy intelligence and intelligence cooperation efforts for detection.

In the area of barter, book-to-book, bulk cash, or currency conversion transactions, countries need to draw on intelligence capabilities and institute or strengthen cooperation with other countries to detect sanctions-circumventing activity and hold violators accountable. This can be done by levying penalties, asset freezes, indictments, or other methods against the actors involved in illicit but opaque financial activity.

9) Governments should better regulate the activities of cryptocurrency exchanges and use intelligence to identify and prevent emerging illicit payment methods

In the realm of illicit finance, governments are at a serious disadvantage where virtual methods of payment are used, such as cryptocurrency or CVCs. For cryptocurrency, governments need to better regulate (or institute basic regulations altogether) the activities of exchanges whose actors or entities operate on their territories. These exchanges should be made subject to standard national laws and regulations on anti-money laundering, reporting, and complying with sanctions and due diligence efforts. Since these exchanges are regularly used for illegal payments, privacy concerns for those entities' customers cannot be placed above preventing criminal activity. The United States is leading the development of regulations in this area and should share lessons and best practices with other likeminded nations.

10) Financial institutions should erect adequate cyber defenses

Financial institutions, particularly those in developing countries and emerging banking hubs, need to institute better cyber defenses to prevent against electronic thefts. As North Korea

successfully pioneers this activity, governments should expect that additional rogue or pariah nations will follow suit. The U.S. government could assist developing nation banks and share ideas on cyber defenses via the Treasury Department.

Preventing the Misuse of Shipping

Not enough has been done to prevent the misuse of shipping to obtain strategic goods. Transshipment of ill-gotten goods remains a major issue, and the use of front companies, freight forwarders, and free trade zones as intermediaries can create such complexity that it is nearly impossible to track the circuitous route of some illicit shipments to their final destination. Too often, suppliers and governments tolerate such entities as the end-users, instead of insisting on verifiably establishing the actual end-user.

11) Shipping companies should be held to higher expectations worldwide; U.S. government should conduct outreach to the shipping community and other governments on counter-proliferation measures

Shipping companies should be treated like all other companies with regard to illicit trade in sensitive goods. Although they often claim they are not responsible for the contents of the shipment, this cannot become an excuse for turning a blind eye when a potentially unlawful shipment is made or requested. Information about a parcel, sender, or recipient that is inconsistent or otherwise suspicious should be resolved before packages or containers are picked up or sent off, and, if unresolvable, should result in denial of service and reporting to authorities. Overall, shippers and freight forwarders need to take a stronger role in conducting due diligence and reporting suspicious activities to authorities. They need to make clear to illicit procurement networks that they will not tolerate having their services misused for illicit shipments, and that they are willing to change their operating procedures to actively participate in counter-proliferation.

Another example of the lack of adequate attention to counter-proliferation is the existence of open ship registries that incentivize sanctions-evading ships to operate more freely. The United States has improved this situation by holding freight forwarders accountable for deliveries to sanctioned recipients, requiring them to have compliance programs, and strongly integrating U.S. customs and customs data in counter-proliferation efforts. The United States should conduct additional outreach to shippers abroad and to other governments.

As a starting point, shipping entities should train staff on illicit procurement methods, institute electronic methods of checking parcels against banned entity lists, and develop technical expertise to determine whether the senders of packages, their content, intended use, or destinations are unlawful. They should adopt risk-based approaches for inspecting parcels or cargos going to certain countries or common transshipment points. Further, customs, border, air, and maritime enforcement officials can use the data collected by shipping entities and integrate it into intelligence and other data, combining it with more sophisticated analysis to conduct risk-based inspections and investigations.

Sanctions Evasion by North Korea and Iran

12) UN member states should better enforce sanctions on North Korea and add to sanctions designations; UN member states should also seek to detect and prevent new Iranian illicit procurements; The United States and its allies should sanction Chinese entities that facilitate illicit procurement by sanctioned countries

Reporting by the UN Panel of Experts on North Korea established pursuant to Resolution 1718 (2006) shows that numerous UN member states are not enforcing sanctions on North Korea. In fact, the reports provide, in effect, a list of countries that the United States should work with to urge sanctions implementation (and broader strategic trade control implementation). If they do not comply with UN sanctions, the United States should add to its unilateral sanctions against entities that facilitate North Korea's illicit business. It should increase work with allies and partners that will act in response to U.S. pressure, including urging them to carry out asset freezes and inhibit North Korea's illicit banking.

The 1718 Committee under the Security Council is delaying adding to sanctions designations while awaiting results of U.S./North Korean diplomacy. As a result, North Korea is adapting to and circumventing sanctions. In the absence of a clear North Korean willingness to dismantle its nuclear and missile programs, the United States should increase its efforts at the Security Council to spearhead additional designations of entities and individuals involved in sanctions evasion, including in the financial sector. To assist this goal, the UN Panel of Experts requires additional staffing, resources, and assistance from the UN Secretariat to undertake and keep up with investigations into North Korea's growing sanctions evasions. They can be helped by more regular member state reporting and consultations. Their mission is valuable: where key networks are closed down, a large impact is often seen on North Korea's ability to make illicit imports or exports or access funds. The Security Council should also consider a new UN resolution augmenting sanctions if North Korea again tests nuclear weapons or intercontinental ballistic missiles.

This report supports that a growing problem with regard to North Korea is also ship-to-ship transfers and sectoral sanctions evasion schemes facilitated by Russia and China. The United States and its partners and allies should continue to hold Russia, China, and any other involved countries accountable by presenting at the Security Council and to the media photographic and satellite imagery evidence of violations that implicates them in North Korean schemes. This publicity may result in fewer violations.

Supplier countries and companies need to remain vigilant as Iran attempts to violate procurement restrictions, particularly as it reduces compliance with the nuclear deal and continues its missile and conventional military-related procurements in violation of ongoing UN bans.

This report describes in case after case the ways in which Chinese entities act as illicit suppliers, transhippers, and financiers for illicit procurement by sanctioned countries, such as Iran and

North Korea. The United States should augment its recent practice of adding Chinese entities to sanctions lists, banning them from doing business with the United States, and allowing the United States to threaten secondary sanctions against other foreign entities that do not halt business with them. The Chinese government has failed to act to prevent this illicit trade for decades, and a more punitive approach, which targets China's economic bottom line, is overdue.

Shoring up of strategic trade controls overall

While outside the scope of this report, the findings of the Institute's *Peddling Peril Index (PPI) for 2019/2020* indicate that some 120 countries still lack basic export controls in any general sense, fifteen years after the passage of UN Resolution 1540 in 2004, which mandated that countries implement controls to prevent the transfer of goods usable in WMD programs.[4] The United States should continue and expand national programs to assist partner countries in deploying and improving trade controls, including financial controls. It should lend expertise and resources to the 1540 Committee and its Group of Experts for programs that assist lagging countries.

Countries should continue implementing the Financial Action Task Force recommendations, strengthening national legislation and licensing against illicit trade, and enacting stronger due diligence requirements for shipping and financial industries. They should seek better regulations at free trade zones to prevent transshipment of strategic goods, close down the use of front or shell companies on their territories, and prevent freight forwarders and shippers from acting with impunity or being exploited via illicit shipping. National agencies that can provide a two-way exchange of timely intelligence and other data should work closely with customs, border, air, and maritime law enforcement officials to help them conduct more sophisticated risk-based inspections and interdictions.

With transit and transshipment controls in their initial stages of development, or altogether absent in many countries, most nations need to do a great deal more to improve their ability to detect and prevent illicit shipments of proliferation-sensitive goods.

Extradition treaties continue to play an important role in bringing justice to those who engage in illicit trade. The United States should seek additional extradition treaties with key partner countries that would allow it to extradite alleged strategic commodity traffickers to stand trial.

Please see the *PPI for 2017* for additional recommendations on broadly improving global trade controls.[5]

---

[4] David Albright, Sarah Burkhard, and Andrea Stricker, *The Peddling Peril Index for 2019/2020, Institute for Science and International Security,* May 23, 2019, http://isis-online.org/uploads/isis-reports/documents/ThePeddlingPerilIndex2019_POD.pdf

[5] *The Peddling Peril Index for 2017,* http://isis-online.org/ppi/detail/peddling-peril-index-ppi-2017/

Annex to Volume I: Reference List for additional Institute Case Studies illustrating methods and tactics listed in Chapter 13

Albright, David and Andrea Stricker. "Case Study- Canada Prosecutes Company for Possible Nuclear Related Export to Iran." *The Institute for Science and International Security* (April 24, 2014): http://isis-online.org/isis-reports/detail/case-study-canada-prosecutes-company-for-possible-nuclear-related-export-to

Albright, David and Andrea Stricker. "Case Study: Nuclear Traffickers Conspired to Procure High Speed Cameras for Iran from Agent who Supplied North Korea." *The Institute for Science and International Security* (May 19, 2016): http://isis-online.org/isis-reports/detail/case-study-nuclear-traffickers-conspired-to-procure-high-speed-cameras/

Albright, David and Andrea Stricker. "Case Study - Man Charged with Exporting U.S. Goods to Pakistan's Nuclear Program." *The Institute for Science and International Security* (April 14, 2011): http://isis-online.org/isis-reports/detail/man-charged-with-exporting-u.s.-goods-to-pakistans-nuclear-program

Albright, David and Andrea Stricker. "U.S. Busts Iranian Smuggling Scheme Involving a Nuclear-Related Good." *The Institute for Science and International Security* (January 31, 2014): http://isis-online.org/uploads/isis-reports/documents/Kaiga_case_study_31Jan2014-Final.pdf

Albright, David and Andrea Stricker, and Daniel Schnur, and Sarah Burkhard. "Additional Taiwan-Based Element of Iranian Military Goods Procurement Network Exposed." *The Institute for Science and International Security* (May 19, 2016): http://isis-online.org/isis-reports/detail/additional-taiwan-based-element-of-iranian-military-goods-procurement-netwo/

Albright, David, and Paul Brannan, and Andrea Scheel. "An Inside Look: India's Procurement of Tributyl Phosphate (TBP) for its Unsafeguarded Nuclear Program." *The Institute for Science and International Security* (January 28, 2009): http://isis-online.org/uploads/isis-reports/documents/TBP_28January2009_1.pdf

Albright, David, and Paul Brannan, and Andrea Scheel Stricker. "Case Study - Former Iranian Ambassador Arrested in UK for Alleged Iran-Directed Smuggling Scheme." *The Institute for Science and International Security* (February 16, 2010): http://isis-online.org/isis-reports/detail/former-iranian-ambassador-arrested-in-britain-for-assisting-iran-directed-s/20

Albright, David and Paul Brannan, and Andrea Scheel Stricker. "Case Study - Middleman Majid Kakavand Arrested for Malaysia-Based Iranian Illicit Procurement Scheme." *The*

Institute for Science and International Security (February 16, 2010): http://isis-online.org/isis-reports/detail/middleman-arrested-for-directing-malaysia-based-iranian-illicit-procurement/20

Albright, David, and Paul Brannan, and Andrea Scheel. "Profitable and Low-Penalty: Illicit Procurement of Items with Nuclear Applications for Pakistan." *The Institute for Science and International Security* (February 27, 2009): http://isis-online.org/uploads/isis-reports/documents/Pakistan_Procurement_Karni_Khan_27Feb2009.pdf

"Case Study - U.S. Company Charged with Pressure Transducer Sales: Who Were the End Users?." *The Institute for Science and International Security* (May 14, 2012): http://isis-online.org/isis-reports/detail/case-study-u.s.-company-charged-with-pressure-transducer-sales-who-were-the

Coughlin, Christopher and Andrea Stricker. "Case Study: Skilled Procurement Ring Charged in Illegally Obtaining Goods for Iran." *The Institute for Science and International Security* (May 5, 2015): http://isis-online.org/isis-reports/detail/case-study-skilled-procurement-ring-charged-in-illegally-obtaining-goods-fo

Leahy, Bridget and Andrea Stricker. "Case Study: Two Plead Guilty in Pakistan Illicit Procurement Case." *The Institute for Science and International Security* (March 26, 2018): http://isis-online.org/isis-reports/detail/case-study-two-plead-guilty-in-pakistan-illicit-procurement-case

Stewart, Donald and Andrea Stricker. "Case Study - Chinese National Sought High-Strength Carbon Fiber for China." *The Institute for Science and International Security* (March 5, 2014): http://isis-online.org/isis-reports/detail/chinese-national-sought-high-strength-carbon-fiber-for-china

Stricker, Andrea. "Case Study - Chinese National Charged with Illegal U.S. Exports to Pakistani Nuclear Program." *The Institute for Science and International Security* (August 23, 2011): http://isis-online.org/isis-reports/detail/chinese-national-charged-with-illegal-u.s.-exports-to-pakistani-nuclear-pro

Stricker, Andrea. "Case Study: Four Turkish Nationals Indicted in Iranian Import/Export Scheme for Making Illicit U.S. Financial Transactions." *The Institute for Science and International Security* (November 30, 2016): http://isis-online.org/isis-reports/detail/case-study-four-turkish-nationals-indicted-for-making-illicit-u.s.-financia

Stricker, Andrea. "Case Study: Guilty Plea for Charge of Exporting Metallic Powder with Nuclear and Missile Applications to Iran." *The Institute for Science and International Security* (March 23, 2017): http://isis-online.org/isis-reports/detail/case-study-guilty-plea-for-charge-of-exporting-metallic-powder-to-iran

Stricker, Andrea. "Case Study - IRISL and Affiliates Indicted on Financial Conspiracy Charges." *The Institute for Science and International Security* (July 8, 2011): http://isis-online.org/isis-reports/detail/irisl-and-affiliates-indicted-on-financial-conspiracy-charges

Stricker, Andrea. "Case Study: Two Arrested in Iranian Aircraft Parts Trafficking Scheme, Result of U.S. Sting Operation." *The Institute for Science and International Security* (December 7, 2016): http://isis-online.org/isis-reports/detail/case-study-two-arrested-in-iranian-aircraft-parts-trafficking-scheme