Institute for Science and International Security

ISIS REPORT

**January 28, 2009**

# Pakistan's Illicit Procurement of Missile and Drone Equipment Using Multiple Financial Transactions

**David Albright, Paul Brannan and Andrea Scheel**

The Pakistani Department of Defence (DoD) utilizes illicit trading networks to procure controlled, high-technology items for its military programs. The French customs investigations authority, the National Directorate of Customs Intelligence and Investigations (DNRED)[1], provided the following case information to the Financial Action Task Force (FATF)[2] for its June 2008 Proliferation Financing Report.[3] The following case studies are summarized from this FATF report. Some details of the cases, such as dates and names of companies and banks, have been withheld from publication at the discretion of DNRED and the FATF. DNRED also withheld the dates for when these illicit procurements took place. In these cases, items of a sensitive nature usable in missiles and drones were procured by the Pakistani DoD using French companies as intermediaries and suppliers. Some of the items sought by the Pakistani DoD were classified by the French Ministry of Defence as war materiel.

## Lessons

These case studies show three aspects of illicit procurement—the obscured routes of purchase orders, shipments, and financial transactions—used by the Pakistani DoD and its associates to obtain military items. This case study highlights in particular the financial component of illicit procurement schemes, which is often as complex as the movement of purchase orders and shipments through multiple countries. Countries of proliferation concern obtain controlled military items by utilizing multiple banks, in addition to front companies, to obscure a purchase order's origins and conceal an item's end destination.

The use of multiple financial institutions by illicit procurement networks to transfer money effectively creates several layers between the end user of an item and the supplier. Electronic bank transfers, completed in days or even seconds, often leave no immediate trail of evidence for

[1] La Direction nationale du renseignement et des enquêtes douanières

[2] The FATF was established by the Paris G-7 Summit in 1989 in response to growing incidence of international financial fraud. The FATF makes policy recommendations to prevent national and international money laundering and financial crimes. See http://www.fatf-gafi.org/pages/0,3417,en_32250379_32235720_1_1_1_1_1,00.html

[3] See: Financial Action Task Force, *Proliferation Financing Report*, 18 June 2008, pp. 35-42. http://www.fatf-gafi.org/dataoecd/14/21/41146580.pdf

enforcement agents and bank associates to detect as money changes locations several times. The origins of payments can be concealed through indirect transfers and split payments to multinational banks located on several continents. Often, the paths of transactions resemble the branches of a tree as they move from national military programs, through various banking institutions, and finally to the bank accounts of suppliers of controlled equipment.

Because financial transactions occur rapidly, they do not always provide time for authorities to act to interdict transfers to illegitimate end users as do more slow-moving shipments of dual-use equipment. However, some banks employ sophisticated tracking systems to detect and report suspicious transactions in real-time, in particular those that screen transactions against a list of suspicious customers. These systems allow officials to detect suspicious transactions, and to freeze them immediately. In developed countries, banks are subject to strict reporting requirements. During reviews of their transactions, banks have detected suspicious transfers that they then reported to authorities. These discoveries can aid investigations and prosecutions as well as add to the list of suspicious entities in screening systems.

**The Cases**

***Case 1:*** A first instance of illicit trade directed by the Pakistani DoD through a French transit point involved an order placed through a French industrial company for dedicated missile and drone electronic tracking and guidance equipment, manufactured in the United States. Figure 1 displays the routes of purchase orders, shipments, and financial transactions used by the Pakistani DoD and its associates. The representative of a Pakistani purchasing network operating in an unspecified European country first contacted a French industrial company for this equipment. This purchasing network's representative had known affiliation to the Pakistani DoD. The French company did not carry the equipment, but the firm's representative contacted an American intermediary who agreed to place the order with an American manufacturer that built the items. A front company located in the United Arab Emirates (UAE) actually placed the order with the French industrial company on behalf of the Pakistani procurement network.

The electronic tracking and guidance equipment was shipped from the United States to France by air freight, eventually passing through the transit point of Marseille. The French customs authorities never cleared the cargo, and it was exported to the UAE. It is suspected that the equipment was shipped to its final destination in Pakistan (see Figure 1).

***Financial Transfers in Case 1*:** In facilitating payment for the electronic equipment, the UAE front company transferred money to a Dutch bank branch located in Dubai. This money was then sent to the branch of a Spanish banking group located in France. This bank was used by the French industrial company. As seen in figure 1, two banks used by the U.S. company, both located in New York, each received a transfer of money—not from the Spanish bank, but from another French bank also used by the French industrial company, where the money had again been transferred. The transaction that was re-routed in France and the transaction that was split when sent to the New York banks inevitably disguised the origin of the money and gave authorities and bank officials little warning that an illicit financial transaction had taken place.

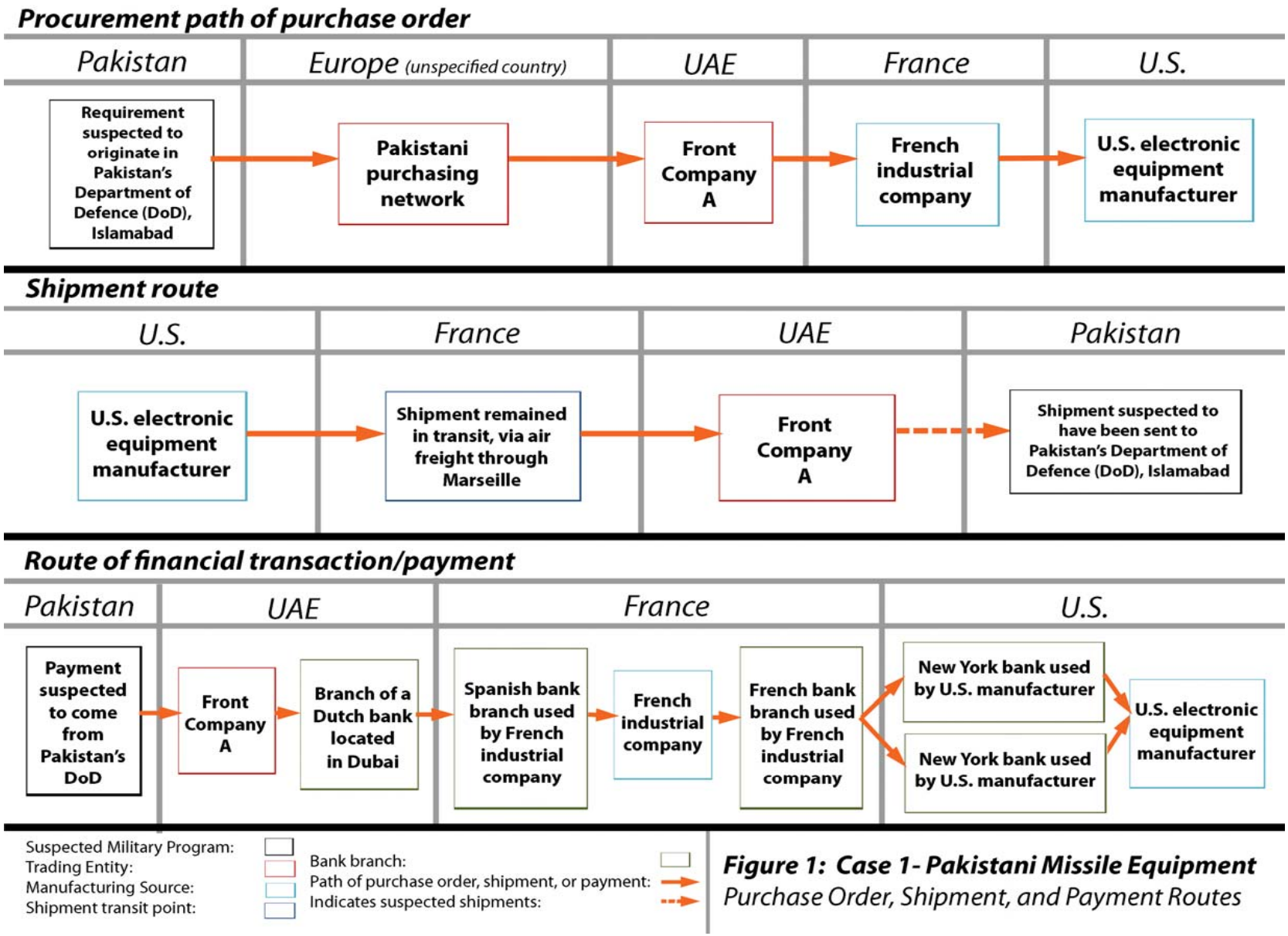


**Figure 1: The routes of purchase orders, shipments, and financial transactions used by the Pakistani DoD and its associates.**

***Case 2:*** A second instance of illicit trade directed by Pakistan's DoD failed in part when one of two intended shipments destined for Pakistan were intercepted by the French customs authorities. This shipment contained highly-sensitive drone and ballistic missile testing and programming equipment. Figure 2.1 shows the paths of purchase orders and shipments used by the Pakistani DoD to procure the targeted items. The Pakistani DoD had placed an order for the equipment through its purchasing network, which operated out of the undisclosed European country. The purchasing network contacted a representative of a small French firm of just three employees, which had expertise in building tracking and fire control equipment for missiles and drones. The purchasing network instructed a Pakistani front company to place 45% of an order for a complete drone calibration and guidance system with this French firm. The purchasing network instructed a UAE front company to place the other 55% of the order. It is unclear whether this front company was the same company used by the Pakistani purchasing network in Case 1 of illicit trade described above. The French firm contacted a Norwegian aeronautics and space supplies manufacturer for additional electronic components it needed to develop the equipment. It is not clear whether the Pakistani DoD knew about the French firm's contract with the Norwegian manufacturer for the electronic components.

The Norwegian parts manufacturer exported the electronic components to France, and the French company exported these and the drone calibration and guidance system, in two separate shipments, to the Pakistani front company and the UAE front company. It is unclear if the two shipments reflected the split nature of the placed orders. The shipments were designated "electrical testing equipment" to customs authorities upon export from France. The Pakistani DoD likely received one of the shipments. The other shipment, bound for either the Pakistani or the UAE front company (it is not clear which), was interdicted at France's Roissy airport. When the French customs authorities discovered the dangerous nature of the technology nearly exported from their country, authorities raided the office of the French firm and the homes of its three employees. The firm was forced to close down operations and faced subsequent legal action. In the course of the investigation, French authorities uncovered substantial involvement of the French firm's director in supplying Pakistan's military programs.

***Financial Transfers in Case 2:*** Figure 2.2 shows the path of financial transactions used by the Pakistani DoD and its purchasing network to facilitate payments to the French, and indirectly, Norwegian suppliers. To facilitate payment for the electronic equipment procured from France and indirectly from Norway, the Pakistani purchasing network utilized two separate financial transaction routes for importing the technologies. The purchasing network sent one transfer of money to its UAE front company, which then sent the money in split transfers to a Chinese bank, and to a Pakistani bank located in Karachi. These transfers were both sent to a French bank used by the French firm. The Pakistani purchasing network specified to the French firm that one part of the sum transfer should be sent to the branch of an American bank located in London, for unknown reasons.

The second route used by the Pakistani purchasing network to facilitate payment for the second shipment of items passed through even more banking institutions than the first route. The network sent the funds through four separate branches of Pakistani banks located in Islamabad, Karachi, Britain, and the United States, and each of these branches in turn made a payment of some portion of these funds to the French bank used by the French firm. Each of these four

branches sent the money via letters of credit to the French bank used by the French firm. The French firm made a financial transfer to the Norwegian manufacturer's bank, located in Oslo, for services rendered.

The Pakistani purchasing network's use of the French bank as the central node for financial transfers assisted the investigation of French customs authorities and helped them to uncover all the transfers associated with payment for the procurements.

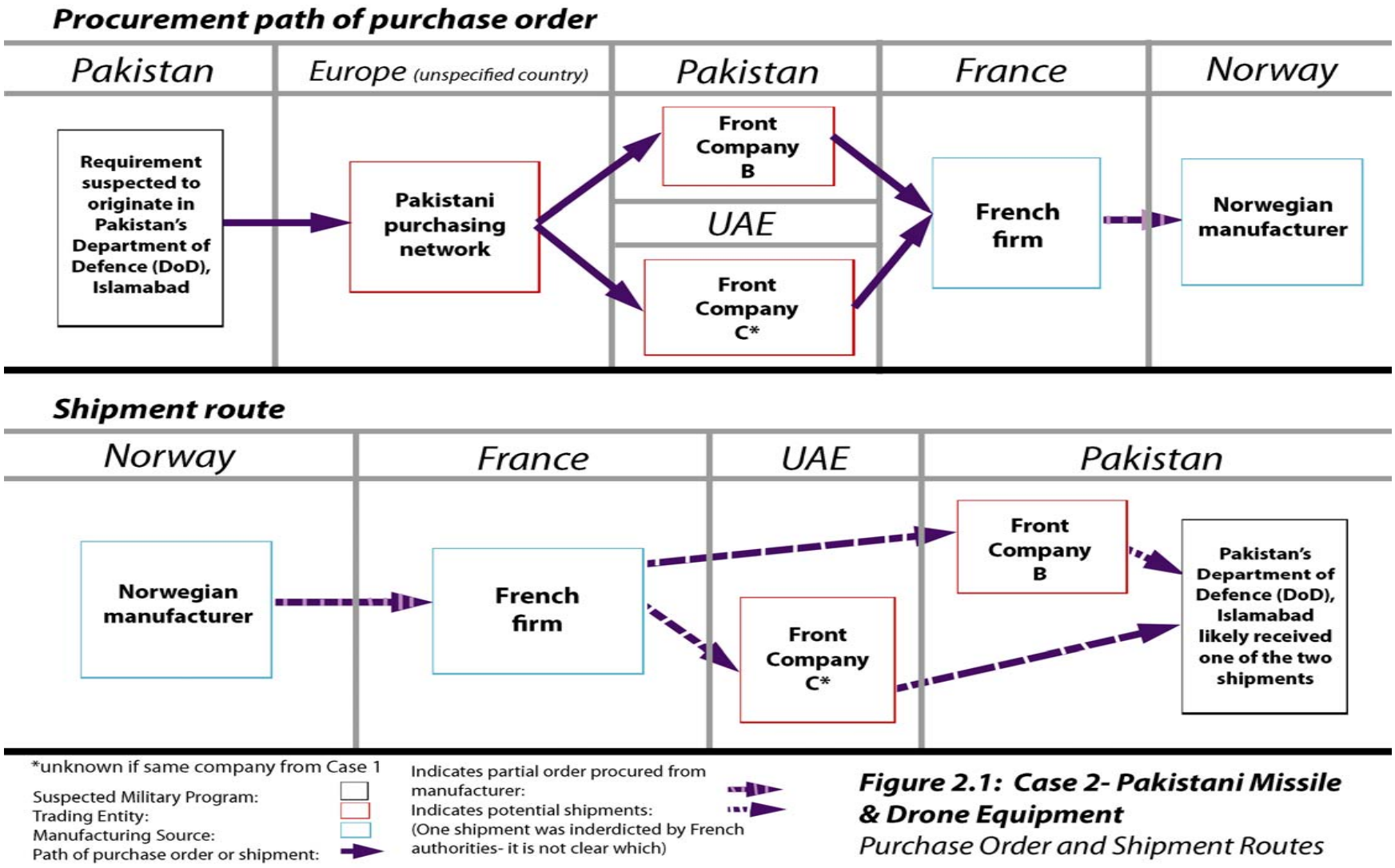


**Figure 2.1: Paths of purchase orders and shipments used by the Pakistani DoD to procure the targeted items.**

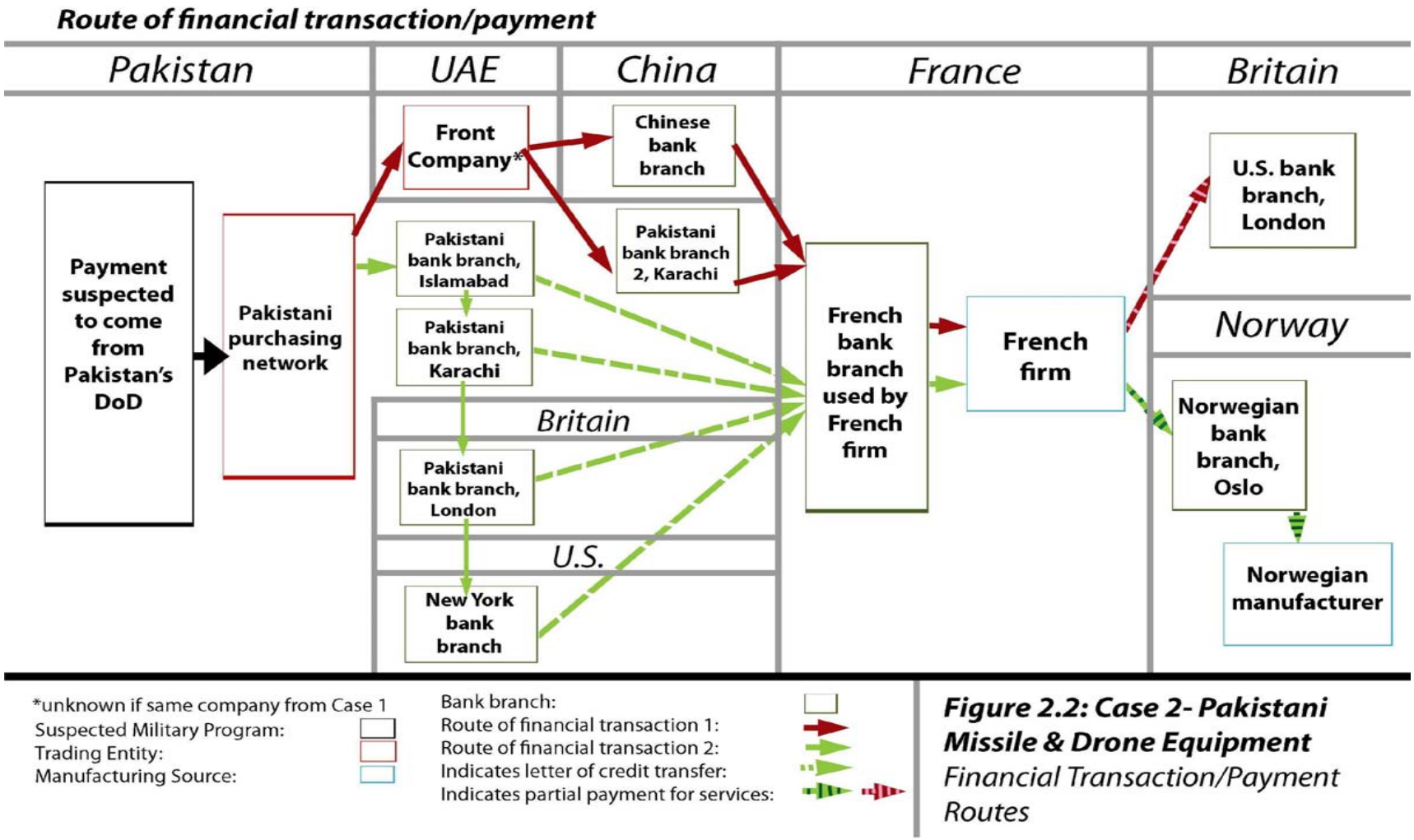


**Figure 2.2: The path of financial transactions used by the Pakistani DoD and its purchasing network to facilitate payments to the French, and indirectly, Norwegian suppliers.**

***Case 3:*** A third case of illicit trade uncovered by DNRED involved the discovery of an illicit trade network directed from French territory by a French industrial company to supply Pakistan's military programs, and the military programs of two other unnamed countries. The French company was directed by an independently operating industrialist, who also oversaw the operations of another company. These companies were two of four firms in the entire world that had the capability to design a particular type of sensitive, dedicated equipment with application to ballistic missiles. The other companies with this capability were located in the United States and Switzerland. Case 3 reveals no specific item procurements or shipments, but showcases the elaborate financial transaction routes used by the French company and its associates to receive payment for items funneled to countries of proliferation concern.

DNRED was able to halt the France-based network when it acted on counterproliferation intelligence to seize a suspected illicit export on its way from Paris' Orly airport to an unspecified country. Once seized, the authorities determined that the items were dual-use articles intended for a ballistics research institution in the unspecified country. The articles were controlled under either war materiel or dual-use distinctions and were thus subject to license. Searches of both French companies' premises revealed that multiple exports of the equipment had already been made to three separate countries, one of which was Pakistan, and that they had consistently been declared non-controlled items upon export. In subsequent legal hearings, the French industrialist admitted knowingly exporting controlled military items and admitted that deception was used to funnel the items.

The legal hearings involving the French industrialist also revealed the network's extensive use of a French front company to conceal its identity as the exporter of items. Intermediaries from abroad often contacted this front company to obtain items from the French industrialist's companies. One of the unnamed countries also used a front company located in Dubai to obtain items from one of the primary French suppliers. The other French supplier was contacted directly for items by a firm located inside Pakistan for items.

***Financial Transfers in Case 3:*** The French authorities uncovered a complex financial transaction scheme used by the French industrialist and his associates to receive payment from the Pakistani DoD and the other two countries for procured items. Figure 3 shows the routes of financial transactions and payments used by the network, facilitated by the use of multiple banking institutions. While some direct payments were made by both Pakistan and one of the unnamed countries to the French companies' banks via letters of credit, the French industrialist also utilized the French front company's bank accounts as transaction hubs. The front company would take a commission of 3% of the sale for its services before transferring the money to a bank accounts used by the French industrialist.

The use of transaction hubs by the network enabled authorities to uncover a massive web of financial transfers, sale relationships, and procurement and shipping routes after they began investigating the network's activities. Without doubt, the use of front companies, in addition to circuitous and layered payment routes, made the France-based network and the other French companies incredibly successful at sending controlled missile and drone technology to Pakistan and two other countries.

**Figure 3 shows the routes of financial transactions and payments used by the network, facilitated in major part by the use of multiple banking institutions.**