



BNL-112333-2016-CP

***Forensic Analysis of Terrorist Counter-Financing to
Combat Nuclear Proliferation***

Bafode Drame, Lisa Toler, Susan Pepper

*Presented at the Institute of Nuclear Materials Management (INMM) Annual Meeting
Atlanta, GA
July 24-28, 2016*

June 2016

Nonproliferation and National Security Department

Brookhaven National Laboratory

**U.S. Department of Energy
USDOE National Nuclear Security Administration (NNSA),
Office of Defense Nuclear Nonproliferation (NA-20)**

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-SC0012704 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Forensic Analysis of Terrorist Counter-Financing to Combat Nuclear Proliferation

Bafodé Dramé¹, Lisa Toler², & Susan Pepper²

1. Dramé International Consulting, Roosevelt Island, NY 10044
2. Brookhaven National Laboratory, Upton, NY 11973

ABSTRACT

Proliferation financing is a new term for the old work of terrorist counter-financing, which is critically important and yet often underappreciated and misunderstood within the nuclear security community. The work of that community is complicated by global politics, regional tensions, the expansion of international commerce, and the emergence of additional nuclear states; all of these factors create new challenges for international safeguards. With confirmed reports of weapons being produced in countries plagued by poverty and corruption, some believe it is only a matter of time before tactical weapons wind up in the hands of the oil-rich Islamic State (ISIS). Further threats come from continuing improvements in advanced isotope separation methods that are both small and difficult to detect. Non-state actors like ISIS therefore pose a threat that is qualitatively different from earlier generations of state-based enemies and massive nuclear warheads. This new threat can be countered effectively only by promoting both a culture of information sharing and good governance by competent local authorities. Such steps are necessary because proliferation financiers currently exploit several cracks in the global financial system as well as a series of difficult-to-implement export controls. Strong empirical evidence links the spread of WMDs to the success of such financiers in working behind the scenes, subverting the best efforts of the international community to stop them. In order to more effectively counteract the threat they pose, the international community will have to recommit to counter-financing efforts, at once one of the most effective, underappreciated, and underutilized tools in the fight against nuclear proliferation. In particular, this paper takes a transactional approach to mitigating proliferation risk, making four key recommendations: (1) fully implement United Nations Security Council Resolution 1540; (2) integrate and standardize the global SWIFT and IBAN systems; (3) improve shipping and trade document verification practices and training; and (4) improve global recordkeeping. By raising awareness of some of the most common deceptive financial practices and the ways in which, by establishing an effective public-private partnership, those practices can be combated more effectively through collaborative international counter-financing efforts, the risk of nuclear proliferation can be reduced even as rogue nations and non-state actors work to increase it.

INTRODUCTION

Nuclear proliferation is almost inarguably the greatest threat facing the world today. The threat of proliferation is increasing in part because of non-state actors (like Al-Qaeda and the Islamic State) that are not obligated to abide by international rules and regulations and in part because of recalcitrant states pursuing nuclear proliferation in an effort to gain national power and prestige. In the latter category is Iran. Despite all of the sanctions imposed upon Iran, the regime in Tehran has made significant inroads toward acquiring materials and equipment for its nuclear program, including the production of enriched uranium. Other threats include North Korea, which regularly uses its nuclear weapons to blackmail the international community, and the Abdul Qadeer Khan (or A.Q. Khan) network, a black-market proliferation network that supplies

nuclear materials to rogue nations. Thus, proliferation is increasing despite the best efforts of the international community to stop it. That increasing threat leaves everyone at risk.

The common denominator in all of these criminal activities is money. Whether in financing proliferation efforts or funding the export of sensitive materials and technology, money is used to sidestep, subvert, or corrupt existing security measures to obtain nuclear materials. In almost every case, money is therefore the single biggest limiting factor determining the success of proliferation efforts.¹ Technological research and development may or may not work. Smuggling efforts may or may not work. If criminals cannot pay for nuclear materials, however, then they do not get them. That leaves financial institutions as the first line of defense in the fight against nuclear proliferation; financial institutions are at the same time the most critical and critically underappreciated tool in protecting the international community.

Perhaps because financial nonproliferation is so underappreciated, it has also been hampered by regulatory gaps and poor collaboration that leave it unable to effectively contend with some of the most common financial practices used by criminals seeking to fund proliferation efforts. This paper will highlight four of the most common deceptive financial practices, explain why they are difficult to detect, and then recommend regulatory changes to increase the ability of the international community to detect, disrupt, and prevent them so that authorities can systematically track and confiscate the dirty money that finances proliferation activities. Particular attention will be paid to the potential for collaboration with shipping companies in implementing tougher export controls with enhanced due diligence (EDD) to limit the flow of dual-use materials to rogue nations and other entities. The specter of nuclear threat is real and constant. Taken collectively, these recommendations stand to counteract that threat, making the world a safer place for all of its citizens.

BACKGROUND

On April 28, 2004, the United Nations Security Council (UNSC) adopted Resolution 1540 to affirm that the proliferation of nuclear, chemical, and biological weapons as well as their means of proliferation constituted a grave threat to international peace and security. The resolution obliges signatory countries to do three things: (1) refrain from providing support of any kind to non-state actors; (2) adopt UN legislation establishing an international nuclear nonproliferation policy; and (3) establish sound import and export controls to ensure nonproliferation. The resolution also encourages information sharing as an essential tool to combat proliferation.

The detection of illicit financial activities and export controls are complementary and mutually inclusive. In 2010, the Financial Action Task Force (FATF) on Money Laundering, an intergovernmental organization founded by the Group of Seven (G7) in 1989 and housed in the Paris headquarters of the Organisation for Economic Co-operation and Development, issued a report titled “Combating Proliferation Financing: A Status Report on Policy Development and Consultation.” That report argued that both tools must be implemented simultaneously to combat proliferation financing. The detection of illicit financial activity allows for the identification and seizure of funds from criminal organizations; export controls, in turn, prevent the illegal transfer of dual-use materials (that is, materials with both commercial and military

¹ For rare states and entities with an indigenous supply of nuclear material, technically competent scientific and engineering personnel, and substantial manufacturing infrastructure, it may be possible to internally finance the pursuit of nuclear weapons development.

applications) and other proliferation-sensitive goods. The FATF report suggests that financial detection measures can reinforce export controls and vice versa.

These tools allow us to combat proliferation financing, but such combat is truly a world war: all countries must cooperate to achieve sustainable success. Unfortunately, the three aforementioned terms of UNSC Resolution 1540 have yet to be fully implemented in many parts of the world: according to the findings of the FATF report, only 80 signatories (out of 192 countries in the world) currently apply proper export controls. Efforts to prevent the proliferation of WMDs have gained momentum in recent years—for example, in 2012, the FATF initiated efforts to promote Non-Proliferation Financing (NPF)—because financial nonproliferation has proven one of the most effective tools in waging this war. Those tools have also proven difficult to use, however, for political reasons: FATF stakeholders could not even agree on a definition of the term “NPF.”

Criminals exploit this kind of confusion by using hundreds of financial tricks to hide or disguise their illegal activities. Four of the most common deceptive financial practices used by proliferation financiers to accomplish their goals include:

- Front companies;
- Outsourcing to offshore jurisdictions with weak export laws or weak enforcement of export control laws;
- Circular transactions; and
- False or incomplete trade documentation.

This paper will survey each of these practices by explaining what they are, how common they are, and why they are difficult to detect, explaining the many parallels between general criminal activity and proliferation financing, and making recommendations about what can be done to combat these practices more effectively.

DECEPTIVE FINANCIAL PRACTICES

1) Front Companies

A front company is any business whose true purpose differs from its advertised purpose, often to divert attention away from criminal activity. “Fronting” is perhaps the most common deceptive financial practice in the world today. It is especially common among so-called “professional” criminal organizations, including arms dealers, drug traffickers, and proliferation financiers. As revealed by the “Panama Papers,” a cache of more than 11 million leaked financial and legal documents, many wealthy people, including heads of state and high-ranking government officials, stash their wealth offshore by investing in dubious foreign companies; the main objective of these investments is to help investors avoid tax payments. Many people associated with such investment companies appear on international sanctions lists.

Front companies can be very difficult to detect. The “Panama Papers” offer a great example: the information contained in many of the leaked documents was subject to attorney-client privilege and could not be legally disclosed. Moreover, in most cases, the fund managers are among the smartest and most sophisticated financiers in the world; they excel at commingling illicit funds with legal investments. One might think that such investment havens would be most common in developing countries, but they are found mostly in Switzerland and other European countries. They are very rare in the United States, where financial regulations are extremely tight. One

clear indication of suspicious activity occurs when a business owner in one industry also owns another business in an unrelated industry and that unrelated business has no clear economic purpose; most often, that business is a front used for money-laundering purposes.

Recognizing that a business with proper documentation has no economic purpose, however, requires consistent and proper training as well as adequate staffing levels. Regulatory authorities must have the education to know what they are seeing and the time to spend looking for telltale signs. Integration of the global financial system would make it easier to accurately monitor the transactions of individuals and companies alike. The continuing implementation of UNSC Resolution 1540, along with other information-sharing efforts and the empowerment of competent local authorities, would also help to corner proliferation financiers, who, in an increasingly collaborative global financial system, would have no place left to hide. Similarly, tighter export controls would prevent the fronting of exports by ensuring that dual-use and sensitive materials are actually used for their declared purpose.

2) Outsourcing to Offshore Jurisdictions

Another common technique of proliferation financiers is outsourcing the administration and supervision of trade finance vehicles to offshore jurisdictions with weak export laws or weak enforcement of export control laws. These jurisdictions tend to be either failed states or regimes with embedded corruption where money can buy practically anything, including the cooperation of governments and competent authorities. All suspicious activities do not happen offshore, nor are all offshore activities inherently suspicious. But most recent global financial scandals have originated in offshore jurisdictions. Just as legitimate entities outsource business to India and China in order to save costs, criminals outsource business to other jurisdictions to evade detection and operate in a comfortably lawless environment. Any sudden move to an offshore jurisdiction therefore creates suspicion. Authorities also rightfully become suspicious when shipping vessels frequently travel to or from high-risk geographic jurisdictions.

In contrast to front companies, it is often not hard to detect offshore activities. Regulatory authorities often know much that goes on there, but they cannot intervene without violating the sovereignty of the other country. Thus, the only remaining options are putting the country on a sanctions list—in which case the criminals often simply move their operations to another country, escaping all harm—or hoping for the criminals to leave the country so that they can be arrested.

By fully implementing UNSC Resolution 1540, establishing broader international information sharing, integrating the global financial system, and empowering competent local authorities to pursue proliferation financiers and their protégés, authorities would no longer be so powerless against criminal activities in offshore jurisdictions.

3) Circular Transactions

Circular transactions are a common form of money laundering. They occur when payments are disbursed to a beneficiary who then sends a similar amount back to the originating party within a short period of time—often as little as a week, sometimes even less—with no apparent business or economic purpose. They may or may not involve front companies or offshore jurisdictions.

Simple vigilance catches many patterns of circular transactions between unrelated parties: for example, what are the chances that a person located in the Sahara does frequent business with someone located in Iceland? It is not hard to detect recurring circular transactions, and many

criminals simply do not know that their methods have been detected until they are arrested. More sophisticated criminals may evade detection, however, with one-off circular transactions.

To catch more of these transactions, it will be necessary to raise awareness of the tactic among local authorities and the general public (and, by extension, among the criminal population) and to increase international information sharing in order to make it even easier for local authorities to see both sides of transactions in which one side purposely takes place in a far-flung corner of the globe.

4) False or Incomplete Trade Documentation

The use of false documentation is fairly self-explanatory, but the range of falsified documents is wide. Among the most commonly falsified documents are vessel or shipping documents to hide the nature, origin, or destination of goods and to evade international sanctions. For shipments going to or coming from high-risk jurisdictions, chances are that some documents have been falsified, especially if illegal merchandise is being transported.

False documentation can be very difficult to detect because it is purposely designed to look like real documentation. Many cases of false documentation are caught when simple inquiries snowball into large-scale investigations, uncovering larger patterns of wrongdoing. Four of the most common types of false documentation practices include:

A) Hiding/Changing Vessel or Container Identifications

If ships or containers are on sanctions lists, criminals often falsify ID “plates” by stealing them from other ships and containers. Customs forms and other documents declaring the contents of a container often misrepresent or outright lie about what they contain. Simple due diligence can catch most instances of such impropriety, but these techniques are generally used in areas where security is lax and manpower is low, making it easier for them to fly under the radar. To prevent such techniques from working, it will be important to create a global information-sharing network, to standardize document formats with anti-counterfeiting features, and to increase training for inspection personnel.

B) Renaming Vessels

Another technique used by proliferation financiers to escape sanctions and avoid drawing attention while smuggling sensitive materials, often on behalf of rogue nations or transnational criminal organizations, is the renaming of a vessel. This technique is not as common, but forged documentation can easily fool poorly trained staff in smaller foreign ports without access to global information-sharing networks. Increased information sharing will therefore help to counteract this method. Further, full implementation of UNSC Resolution 1540 will disincentivize such methods by authorizing the confiscation of such vessels.

C) Falsifying the Cost of Shipments

As shown in Figure 1, another instance of false documentation involves the manipulation of shipping invoices to artificially inflate or deflate the cost of shipments. It is used to launder money and to finance proliferation efforts. It is hard to estimate the frequency of this technique, however, because it often goes undetected. Knowledgeable people are therefore needed to verify shipping documentation. Here again, information sharing is critical. A global network could share not only the names of known falsifiers, but also common patterns of falsification, thereby raising awareness.

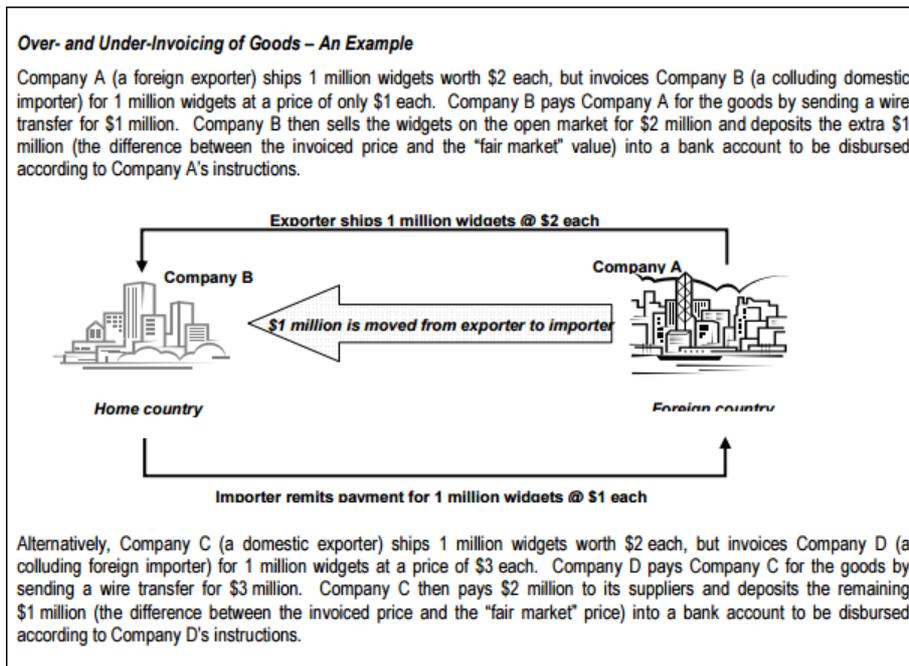


Figure 1: An Example of Shipping Cost Falsification (Source: Financial Action Task Force)

D) Missing Information in Shipping or Trade Documents

Missing information is exactly what it sounds like. Sometimes the originator or beneficiary information is missing. Other times the Originating Bank Information ("OBI") might contain the terms "Cover payment," "Direct cover payment," "One of Our Clients," or "One of Our Good Clients," which automatically raises a red flag. Missing information is one of the most frequently used methods of falsifying documentation because it hides the true identities of the parties involved. In other cases, vague descriptions of cargo hide its true contents: for example, gun shipments are sometimes described as "machined parts." Though it is easy to see when information is simply not listed, sometimes omissions happen because of an oversight or an innocent system glitch. Proliferation financiers purposely seek to give the appearance of such technical difficulties to avoid suspicion. Vague descriptions are even harder to catch because the fields are not blank; instead, what is missing is specificity. There are no legitimate purposes for missing information, however, and good investigators can thus easily distinguish between genuine glitches and instances of purposeful deception or wrongdoing when their follow-up investigations encounter roadblocks. Proper education of shipping verifiers is therefore critical—especially since criminals rapidly adjust to any changes in security practices, creating a perpetual arms race. Document verification would also be made significantly easier with increased global information sharing.

RECOMMENDATIONS

In the foregoing descriptions of common deceptive financial practices employed by proliferation financiers, several themes emerge about the sorts of changes needed to counteract those practices more effectively. This paper offers four main recommendations:

1) Fully Implement UNSC Resolution 1540

In order to create a cooperative international community that works together to combat the threat of nuclear proliferation, it is necessary that each country affirms its commitment to the common

cause by fully implementing the aforementioned terms of UNSC Resolution 1540. That step would also help to disincentivize some of the practices described above.

2) Integrate Global Information-Sharing Networks by Extending SWIFT and IBAN

During an international financial transaction, a Society for Worldwide Interbank Financial Telecommunications (SWIFT) code identifies a specific bank whereas an International Bank Account Number (IBAN) identifies an individual account. The IBAN system is used mostly in Europe and not in the United States, where American Bankers Association Routing Transit Numbers are used instead. The United States relies heavily on the SWIFT system, however, particularly when requesting or sharing information about transactional activities.

The use of multiple separate tracking systems necessarily limits and weakens global information-sharing efforts. The IBAN system is meant to collect specific information on individuals and their transaction histories; SWIFT does the same for banks and organizations. Implementing and standardizing these two systems would allow for coherent information sharing, an essential tool for combating money laundering and terrorist financing and verifying sanctions against rogue nations and non-state actors, thereby mitigating nuclear proliferation risk. These steps can save lives without interfering with state sovereignty.

3) Improve Document Verification Practices and Training

Technology is a great enabler in the fight against proliferation financing, smuggling, money laundering, and other illicit activities. Electronic systems are designed by people, however, and they can always be fooled by people determined to circumvent them. That is why document verification by humans is a necessary supplement to electronic screening. Document verification agents must receive frequent and consistent training to remain current on developments in the field and ensure that they are observing EDD practices. Electronic alerts are useful to raise red flags, but false positives can and do happen. Similarly, illicit behavior can elude electronic detection. Trained human agents must reconcile all alerts while remaining vigilant for other sorts of threats as they develop.

4) Improve Recordkeeping to Inform Training and Information-Sharing Efforts

Recordkeeping can be critical in vetting clients and vessels for past illicit activities and risk of future activities, but specific requirements for recordkeeping and retention vary widely. In some jurisdictions, records must be maintained for up to five years. In others, records are discarded much sooner if they were ever kept in the first place. Records are an indispensable part of global information-sharing efforts. To make those efforts as effective as possible, it will be important to improve the quality of recordkeeping around the world as well as to increase legal requirements concerning the length of time for which those records must be maintained. Such records will assist in sanctions list verifications, enforcement of export controls, and integration of the global financial system, among other critical tasks.

CONCLUSION

Strong empirical evidence links attempts to acquire nuclear weapons technology, materials, and equipment to the behind-the-scenes efforts of proliferation financiers who work hard to subvert the international community's best efforts to stop them. In order to counteract the threat they pose more effectively, the international community will have to recommit to counter-financing efforts, at once one of the most effective, underappreciated, and underutilized tools in the fight against nuclear proliferation. In particular, this paper makes four recommendations: (1) fully implement UNSC Resolution 1540; (2) integrate and standardize the global SWIFT and IBAN

systems; (3) improve shipping and trade document verification practices and training; and (4) improve global recordkeeping. All four of these policy-level changes are critical to the fight against nuclear proliferation, but policymaking alone will not change the situation. There must be cooperative information sharing and a universal embrace of principles such as those espoused in UNSC Resolution 1540. Local governments must also empower competent local authorities to implement these policies. Stronger reporting requirements for financial institutions would help, as would harsher penalties for financiers: since they already operate outside the bounds of the law, blacklisting is no deterrent. Systemic change, however, takes time. This paper aims to raise awareness of some of the most common deceptive financial practices and the ways in which, by establishing an effective public-private partnership, those practices can be combated more effectively through collaborative international counter-financing efforts, thereby reducing the risk of nuclear proliferation even as rogue nations and non-state actors work to increase it.