Points of Deception: Exploring How Proliferators Evade Controls to Obtain Dual-Use Goods

GLENN ANDERSON

Abstract

This paper examines the question of how proliferators go about evading nonproliferation controls to obtain dual-use goods. It argues that the proliferator must determine a suitable ‘point of deception’ for proliferation to succeed. Some of the factors involved in determining this point are outlined. The use of ‘points of deception’ in procurement for the nuclear and missile programs of several countries is considered. The paper concludes by considering how nonproliferation controls can best address the risks identified through the points of deception model.

Keywords

Nonproliferation, procurement, illicit trade, smuggling, nuclear, export controls, strategic trade controls

Introduction

This paper examines the methods by which proliferators carry out illicit procurement to obtain dual-use goods for use in nuclear weapons and missile delivery system programmes. Since the entry into force of the Nuclear Nonproliferation Treaty in the 1970s and the creation of the Nuclear Suppliers Group, the ability of states to proliferate by procuring complete facilities from international suppliers has been significantly reduced. There continue to be the occasional exceptions, such as Syria’s acquisition of a nuclear reactor from North Korea in the late 2000s, which was almost completed before Israel acted to destroy it.2 However the general trend is clear: states generally cannot procure complete facilities outside of International Atomic Energy Agency (IAEA) safeguards.

Consequently proliferators have generally changed tack, with the focus of procurement shifting towards the component and material level, and towards obtaining technology (both tangible technology and intangible ‘know-how’) that furthers their capability to manufacture such items for themselves. Many of the ‘dual-use’ goods sought have been either not included in export control lists or, although listed, also had plausible

1 Glenn Anderson is a research associate at Project Alpha within the Centre for Science and Security Studies at King’s College London.
benign uses which could allow an export license to be granted. In some cases good have simply been smuggled to avoid controls altogether.

Of interest to this paper is the question of how it is that determined proliferators have been able to forward their programmes despite the increasing coverage of controls since the 1970s. Specifically, this paper explores what could be the considerations of a proliferator when planning a procurement. It is argued that the procurer’s prime task is to successfully set at least one “point of deception,” which is the point at which the details of the true end use or end user of the goods to be procured becomes obfuscated. Upstream of this point, there are entities that are consciously working to a proliferator’s agenda, and seeking to deceive, suborn, persuade or manipulate those entities downstream into acting in such a way that a procurement objective held by the proliferator is met. Immediately downstream there may be only innocent parties, ignorant that there is anything illicit going on, or there may be entities that are aware that the business is illicit.

This paper builds upon the observation of the author that the procurement efforts of different programmes have often utilised similar approaches over the last four decades. For example, Pakistan was perhaps the first country to systematically utilise illicit procurement methods on a large scale to procure goods for its nuclear programme after international counter-proliferation controls were introduced following the Indian ‘peaceful nuclear explosion’ in 1974. Iraq’s nuclear programme also utilised clandestine procurement techniques extensively in the 1980s to procure goods. The use of clandestine procurement and illicit trade techniques by the Abdul Qadeer Khan network has been extensively analysed. It is notable that the customers of A.Q. Khan, both before and in some cases after interaction with the network, relied extensively on their own clandestine procurement networks. Libya, for example, had a clandestine nuclear programme before being offered the Pakistani designs and subsequently maintained a parallel capability to procure technology and materials for its missile programme. Less is known about the procurement channels used by North Korea, but it is certainly the case that the North Korean nuclear programme has relied extensively on illicitly procured dual-use technologies for the decade since the Khan network was dismantled. Since the unravelling of the Khan network, however, it was perhaps Iran that utilised illicit procurement techniques with most vigour, with Iran’s president admitting to the use of such techniques in 2014 because he saw sanctions as illegitimate.

3 ‘Dual use’ goods are goods that can be used for both civil and military applications. They can range from materials to components and complete systems, such as aluminium alloys, bearings or lasers. Definition derived from guidance at <www.gov.uk/controls-on-dual-use-goods>.

4 Illicit trade occurs when states or other entities use deceptive and fraudulent methods to circumvent export controls and sanctions to obtain the goods and services that they need to sustain their WMD efforts.


6 For example, see account in Graham S Pearson, The UNSCOM Saga (New York: Palgrave MacMillan, August 2000).


11 “Iran President Rouhani Hits out at U.S. Sanctions,” BBC News, August 30 2014.

In exploring the ‘point of deception,’ a three-part process is hypothesised. The first phase relates to understanding the targets from whom goods can be obtained. The second relates to the ways by which goods can be acquired from the target – i.e. the provider of goods, normally a commercial company in the business of manufacturing or supplying the goods concerned. The third relates to the techniques that proliferators can use to avoid raising the attention of the government under whose export jurisdiction the provider sits, and to avoid interruption by international counter-proliferation actors such as foreign intelligence services.

The paper argues that gaining an insight into the various ‘points of deception’ presents nonproliferation opportunities. In fact, it may be that a ‘point of deception’ is one of the places in which an illicit procurement network is most vulnerable. If the party being deceived can see through the ruse then they would be strongly positioned to gain insights into the network, and may be motivated to work with nonproliferation authorities to exploit these insights in order to thwart the proliferator’s procurement objectives. It may also result in the existence of a hitherto unknown illicit programme being uncovered.

This paper proceeds as follows. First, the point of deception framework is set out and its elements developed. Next, the paper examines the points of deception routinely used in procurement for the nuclear and missile programs of Pakistan, Iraq and North Korea. Finally, consideration is given to what insights the points of deception framework gives to improve nonproliferation controls.

**Nonproliferation Controls**

Since the beginning of the nuclear age, efforts have been made to prevent proliferation through international trade. The early efforts were introduced alongside the Atoms for Peace initiative which was announced in 1953. This principally involved IAEA safeguards intended to prevent the supplied technologies being misused. The nature and scope of Atoms for Peace era controls was insufficient to prevent the misuse of nuclear technology, however, as was vividly demonstrated by India’s “peaceful nuclear explosion” in 1974. India, a country that had not signed the Nuclear Nonproliferation Treaty, had accepted only basic safeguards to ensure that nuclear materials supplied from overseas could not be used in a nuclear weapon: these measures did not prohibit India from utilising foreign-supplied facilities to produce its own fissile material for use in the nuclear explosion or from conducting the explosion for peaceful as opposed to military ends.13

In parallel to the efforts of states like India to advance their nuclear programmes for military ends, supplier states were beginning to take measures to curb proliferation based upon imported materials and technologies. The first effort in this regard was that of the “Western Suppliers Group” in the 1960s.14 A second initiative was the Nuclear Nonproliferation Treaty which was negotiated after China’s nuclear test in 1964 and which eventually came into force in 1972. The next major initiative was the creation of the Nuclear Suppliers Group (NSG) in 1975-1978 which sought to produce even more detailed lists of technology and agreement on more stringent rules for their transfer.

By the late 1970s, then, the key elements of the nonproliferation toolset, as viewed today, were in place. However, there were still limitations that would be exploited. These included the failure of the NSG to agree to controls on “dual-use” technologies (which were referred to as “grey areas”) during negotiations in the 1970s.15 These challenges were gradually addressed in the decades that followed, particularly after the discovery of Iraq’s substantial clandestine nuclear infrastructure following the first Gulf War.16 However,

---

15 A file on the subject of “grey areas” left over from the NSG discussions in the 1970s was found in UK national archives. FCO96/991: Nonproliferation “Grey Areas,” UK National Archives, Kew Gardens.
16 See, for example, “Press Statement of Nuclear Suppliers Meeting: Meeting of States Adhering to the Nuclear Suppliers
one substantial gap that remained was related to coverage of controls: the Nuclear Suppliers Group had seven original participants which quickly increased to fourteen in the 1970s. By the time Iraq’s programme was uncovered in 1991, this had risen to twenty-six. However, there were still numerous states that had no controls in place at all. The proliferation ring of A Q Khan, which sold enrichment capabilities to several states, exploited this loophole and also procured from countries with weak export controls to facilitate its illicit activities. However, it also succeeded in procuring illicitly from countries with stronger controls. The adoption of United Nations Security Council resolution 1540 in 2004 provided the final substantial addition to the nonproliferation toolset, making implementation of nonproliferation controls a requirement of all states under Chapter VII of the UN Charter.

Evasion of Controls

Despite the increasing coverage of controls, it is apparent that several states have been able to advance clandestine nuclear programmes over the past 30 years. Individual procurements will be examined further in the next section, but for now it is useful to highlight the extent to which illicit procurement methods have been utilised to forward such programmes.

Table I: Illicit Procurement Programmes

<table>
<thead>
<tr>
<th>Country</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pakistan</td>
<td>Mid-1970s – present decade</td>
</tr>
<tr>
<td>Iraq</td>
<td>Mid-1970s - 1991</td>
</tr>
<tr>
<td>Iran</td>
<td>Mid-1970s – present decade</td>
</tr>
<tr>
<td>Libya</td>
<td>1969 - 2003</td>
</tr>
<tr>
<td>North Korea</td>
<td>1960s – present decade</td>
</tr>
</tbody>
</table>

The scale of the materiel need for a nuclear programme is immense, meaning that it is typically not one but hundreds of procurements that are required. For example, a centrifuge cascade, which typically consists of 164 or more centrifuges, likely requires several hundred or more individual components – from metal tubes to precision electronics. Evidently, the technique used for each individual procurement will vary depending on a variety of factors. These may include the control status, sensitivity, and commercial availability of the goods being sought – some goods are more closely watched by international authorities than others. The timescale in which the item is required is also a factor. Another is whether a programme is already viewed as being of concern across the international community, or whether detection of the procurement is likely to result in it becoming so.


17 An example of how the Khan network benefitted from such a lack of controls is given by the Malaysian police report which concluded that no Malaysian laws were broken when large numbers of centrifuge components designed for uranium enrichment were manufactured in Malaysia by private company SCOMI and shipped secretly to Libya (Polis Diraja Malaysia, “Press Release by Inspector General of Police in Relation to Investigation on the Alleged Production of Component’s for Libya’s Uranium Enrichment Programme,” 20 February 2004).


19 The Libya case differs from the other cases mentioned in Table I as Libya procured an entire infrastructure from the Khan network. It was the Khan network, rather than the Libyan state, that sought the materials and components through hundreds of individual transactions.

20 Pakistan and Iraq at various times have apparently not been of high concern in real terms to senior Western policymakers (at least in the US) because of geopolitical issues that trumped proliferation concerns. See Catherine Scott-Clark and Adrian Levy, Deception: Pakistan, the United States, and the Secret Trade in Nuclear Weapons (London: Atlantic Books, 2007).

21 For example, given the nominally peaceful nature of the Iranian nuclear programme and the high degree of scrutiny the
Clandestine Procurement Techniques: The Points of Deception

In the absence of an ability to procure goods overtly, proliferators must procure goods illicitly. In illicit procurement, a party – be it the exporter, the licensing authority, or some other party, must be deceived. Conceptually, there appear to be three tasks for a proliferator when designing a point of deception. The first concerns where to procure the goods – herein called ‘targeting.’ The second is how to approach the supplier. The third, assuming that the exporting state is not complicit in the transaction (else the procurement would be overt rather than clandestine) is that of evading the export authority.\(^\text{22}\) Additionally, there will be on-going enabling activity involving development and maintenance of procurement networks and their associated infrastructure, and protecting them from detection/disruption by national and international authorities. These four elements make up the “points of deception” framework and are explored in turn below.

**Targeting**

The first step in the process of setting a point of deception is to identify from where the items can be sourced. As the goods required can usually be procured via ordinary transactions with commercial suppliers, for the most part, this activity often amounts to the same market research that a licit procurer would carry out, using standard commercial information sources and contacts in the trade. In practice, there is a relatively small manufacturing base for most proliferation-sensitive goods, although some of these goods can be sourced through global supply chains.\(^\text{23}\) In some instances the procurer might be able to identify opportunities to obtain certain goods from non-conventional sources of supply, such as black marketeers or illegal counterfeit manufacturing operations.\(^\text{24}\) Another possibility is to identify companies or individuals who have the ability to manufacture the items, even though they would not normally appear to be suppliers for these goods.\(^\text{25}\) An additional possibility is to identify an organisation that is a user of the goods being sought, that might be prevailed upon to sell those goods to the procurer. This may be particularly likely to succeed if the goods have been legitimately exported from their country of origin to a customer located in another country, where export controls are less developed and there is a generally lower risk to the illicit procurer. Re-export to the end destination, possibly via one or more intermediary countries to reduce the chances of detection, can then be carried out. Of course, an alternative would be to proactively seek out someone with a credible legitimate end use for the goods in question in such a third party country, and persuade them to purchase the goods from a supplier country with the ultimate (hidden) objective of selling them on.

Traditionally, targeting may have included the use of trade directories and cold calling in the absence of specific knowledge of potential suppliers.\(^\text{26}\) In the era of the internet, this task is changing: online trading platforms such as alibaba.com have often made the process of finding a vendor for desired items much simpler and have facilitated speedy transactions. To some extent, industry and market knowledge, and access to relatively expensive reference resources (such as the hardcopy directories of equipment and

---

\(^{22}\) Overt to the involved elements of the government in the supplier country, that is. The procurement could still be clandestine with respect to the rest of the world.


\(^{24}\) As an example of the potential issue, an examination of the increasing problem of counterfeit parts in the aerospace industry is given in “Counterfeit Parts: Increasing Awareness and Developing Countermeasures,” Aerospace Industries Association of America, 2011.<http://www.aia-aerospace.org/assets/counterfeit-web11.pdf>

\(^{25}\) For example the manufacturing of centrifuge rotors for Iraq in the 1980s by the German company Rosch, whose usual line of business was carbon fibre products for the automobile, aircraft and computer industries. Rosch was owned by Karl Heinz Schaab. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

\(^{26}\) An associate of A Q Khan’s, Abdus Salam, reportedly connected with businessman Peter Griffin when misdialling a cold-call to a firm. See Catherine Scott-Clark and Adrian Levy, *Deception: Pakistan, the United States, and the Secret Trade in Nuclear Weapons* (London: Atlantic Books, 2007).
suppliers that once featured prominently) are now of significantly less importance, and a greater number of individuals can attempt to conduct procurement for technical items in an economical fashion with a reasonable chance for success, although this is probably less the case when it comes to acquisition of the most specialist and distinctive items with nuclear applications.27

The perceived strength of nonproliferation controls in each supplier’s country and the risk that any specific transaction is a sting operation could affect the choice of target. In this context, it is notable that countries such as Iran prefer US and European-origin goods but often seek to procure them via countries such as China, which is perceived to have a less robust export control system.28,29

**Approaching the Supplier**

The proliferator must carefully consider how to approach a supplier as, depending on the nature of the procurement, it could result in the programme being detected (if it has remained hidden up to that point) or the procurement channel being compromised. For example, it was an approach to the UK company Emerson Industrial Controls for frequency inverters by the Special Works Organisation in Rawalpindi, followed by a subsequent message from the purchaser asking for technical modifications, which resulted in the UK concluding that Pakistan was pursuing uranium enrichment by centrifuge, likely in support of a nuclear weapons programme.30 In general, in any illicit transaction, the supplier can either consent from the outset, be suborned or be manipulated. These scenarios are explained below.

An additional possibility is theft from the supplier. Although cases of theft of goods from suppliers appear to be relatively rare for proliferation purposes, there have been a number of cases where a mixed methods approach is used: an insider is co-opted who then, in effect, commits an act of theft against his employer. One example of this is the case of Sihai Cheng. Cheng was indicted by the United States in 2013 and charged with facilitating the diversion of MKS-brand pressure transducers from the company’s Chinese subsidiary to Iran’s nuclear programme. It is alleged that Cheng worked with sales staff of the subsidiary to have the goods shipped to intermediary counties for onward export to Iran while the sales staff declared the sales to be for existing and new customers.31

**Consent (Whether Informed or Given in Ignorance)**

**Informed consent:** In some instances, the procurer may turn to a provider who he already knows (or has good reason to expect) can be made aware from the outset of the true nature of the proposed deal. This situation may arise because the provider has been used before by the procurement network, they have information that the provider has been used by another illicit procurement network in the past and the situation is comparable, or because the provider has been ‘scouted’ by someone who has established their

---


willingness to provide goods illicitly, prior to any specific request.\textsuperscript{32}

**Ignorance:** The possibility that a supplier is simply ignorant of export controls and/or proliferation risks (be it true ignorance or wilful blindness) should not be discounted. In such circumstances, a proliferator could approach a supplier without subterfuge, or using only a very small amount of subterfuge and obtain the goods.

Working with consenting suppliers may be attractive to proliferators as in some respects it reduces the need for subterfuge. However, deception would still be necessary to evade national controls, as explored below. Additionally, a consenting partner may increase their prices because of the increased risks involved.

**Subornment of Supplier**

At times, the procurement network may try to suborn an individual, or individuals, outside the existing network.\textsuperscript{33} For instance the buyer may not believe that the supplier can be put at ease with deception about the end-use of the goods. This may occur for a number of reasons, for example if the procurement requirement demands particular specifications that will give clues as to the real end-use.\textsuperscript{34} In such a case the procurers may try to suborn the appropriate person or persons in the supplier company into conspiring with them.

As well as enabling the procurement of goods from any supplier organisations they may belong to, suborners may be invaluable in approaching other suppliers (particularly when these can then appear to be unremarkable domestic enquiries from fellow nationals or the suborned individual or their company is well known in the industry), in the evasion of export controls, avoiding the attentions of investigative/intelligence agencies, etc. and arranging financing and other services. Suborners may also help in obtaining training, maintenance, technical information, and the benefits of empirical experience in a particular field including hard-to-capture tacit knowledge.\textsuperscript{35}

There are a variety of ways in which an individual can be suborned. Generally, these align with the motivations through which an intelligence service may persuade an individual to give them access to information. These are often held to be chiefly financial reward, ideological reasons, self-esteem and/or excitement, and revenge (although a number of other factors, including some subtle aspects of interpersonal relations, can often play a key role, and are arguably sometimes the decisive factor).\textsuperscript{36} A key ability for the procurer will be to identify who might be suborned to meet their ends, and identify what characteristics, objectives, desires and vulnerabilities a target for subornment may have, which can be exploited.\textsuperscript{37} Thus the first part

\textsuperscript{32} An example of this is the use of a French businessman, alias ‘Jaques Rough’, to help acquire maraging steel for the Iraqi centrifuge project in the 1980s. Rough was already involved in less clandestine procurement for Iraq’s conventional arms industry. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

\textsuperscript{33} Subornment is an activity in which an illicit procurer persuades or induces a person (or persons) outside the illicit procurement network to become complicit in illicit activity in order to help achieve the procurement goals.

\textsuperscript{34} For example in the procurement of 350-grade maraging steel by the Iraqi gas centrifuge project in 1988, the procurers were unable to come up with a credible cover story regarding the use the steel would be put to, and so went directly to a black market dealer. This dealer (‘Malik’) had been located for them by an intermediary that had been working with the Iraqi government for some time and who was aware from the outset that the deal would be illicit. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).

\textsuperscript{35} The contribution to overcoming Iraqi problems in balancing developmental centrifuges made by Karl Heinz Schaab illustrates the importance of the tacit knowledge that key suborners may contribute. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).


\textsuperscript{37} For example the co-opting of German engineer Bruno Stemmler by the network procuring for Iraq’s clandestine gas centrifuge programme in the 1980s. See Obeidi and Pitzer, *The Bomb in My Basement* (New York: John Wiley & Sons, 2004).
of the subornment task overlaps with areas within the Targeting activity discussed above.

Once the target has been identified, the next hurdle will be the actual act of subornment, which may rely heavily on the abilities (such as interpersonal skills) of the individual tasked to undertake it. Once a target has been successfully suborned, managing that relationship and getting the results desired, whether for a one-off deal or on an on-going basis, presents additional challenges.

Subornment can be a high risk operation: if it goes wrong, the suborner’s cover can be compromised and, in some cases, criminal prosecutions could result.\(^{38}\) Even if subornment is successful, there remains a risk that at a later stage a suborned individual will have second thoughts, or be uncovered by uncorrupted colleagues, business contacts or the authorities, leading to them either being exposed or secretly ‘turned’ to work for the authorities.\(^{39}\) There is also the risk that those targeted have already been enlisted to assist the authorities, and have in fact been working against the procurement network from the outset.

Another potential disadvantage of using subornment is cost. Those suborned are likely to want financial inducements in exchange for cooperation.\(^{40}\) There is also the issue of the time and effort put into the initial subornment and subsequently handling that contact. This could be substantial, particularly if a suborned individual proved to be malicious, unstable or incompetent, or began to have worries over their illicit dealings.

Nevertheless, there are circumstances where it is likely to be very difficult, if not impossible, to meet specific procurement requirements without some degree of subornment.\(^{41}\) In addition, a successful subornment can provide great benefits to an illicit procurement effort, particularly if the individual or individuals concerned are reliable and stable, discreet, capable, knowledgeable in their field, well-connected and have initiative.\(^{42}\)

\textit{Supplier Manipulation}\(^{43}\)

For the majority of illicit transactions, the provider will probably neither knowingly consent nor be suborned. Instead, they will be manipulated through the provision of false information, or misled with incomplete information.\(^{44}\)

---


\(^{39}\) For example, the reported recruitment of members of the Tinner family, part of A.Q. Khan’s procurement network, by the CIA. See Collins and Franz, \textit{Fallout} (New York: Free Press, Simon & Schuster, Inc, 2011).

\(^{40}\) Financial motivations were key to the assistance provided by the owners of H&H Metalform to Iraq (see Obeidi and Pitzer, \textit{The Bomb in My Basement} (New York: John Wiley & Sons, 2004).

\(^{41}\) Subornment may be required in situations where the specifications of materials or equipment required are so particular that they strongly indicate that the items are desired for an illicit end-use, particularly where there are few (if any) credible legitimate end-users for such items, and the buyer cannot convincingly present themselves as representing one of these possible end-users. Quantities required may also make it difficult to mislead any supplier over the actual end-use intended for the items. In such situations attempting to deceive or manipulate a supplier is unlikely to be feasible, and their witting assistance of illicit acquisition will be needed. An example of a situation where a credible cover story could not be manufactured and reliably maintained, and the procurers instead had to identify a supplier who would be willing to engage in illicitly supplying material while effectively conscious of the real end use, is given in Obeidi and Pitzer, \textit{The Bomb in My Basement} (New York: John Wiley & Sons, 2004).

\(^{42}\) One example of such a high value individual is Peter Hinze, of German company H & H Metalform, who accepted an offer of a ‘silent partnership’ and funding from Safa Habobi, a senior figure in Iraq’s clandestine procurement efforts, in the 1980s. Hinze went on to facilitate cooperation by many companies with whom he had relationships and Iraq’s illicit procurement campaign. See Obeidi and Pitzer, \textit{The Bomb in My Basement} (New York: John Wiley & Sons, 2004).

\(^{43}\) I.e. where the provider of the goods is manipulated, including the use of deception aimed at the provider.

\(^{44}\) There are many examples where goods ostensibly destined for a civil purpose have been diverted to proliferation-related uses. In 2003, the Australian government prohibited an Australian firm, GBC, from exporting a dual-use mass spectrometer to Iran.
The two key areas in which a law-abiding supplier is typically deceived relates to the real end-use for the goods and the identity of the real end-user. In some circumstances, deception about either one or the other may suffice, but usually the procurer will need to deceive the supplier on both scores. The declared end use for the goods would usually have to be consistent with the nature of the business that purports to be the true end user.\footnote{45}

This type of deception is a common tactic.\footnote{46} It can be an inexpensive option as there is no need to suborn suppliers or pay a risk premium for their products or services. However, the cost and complexity of establishing credible \textit{bona fides} can be substantial, particularly if they are to deceive the national authority too.

One particular strategy that has been seen in practice has involved manipulation of suppliers into thinking that a sale is not for export when in fact it was. This technique often involves a third entity in the country, be it a credible customer or a freight forwarder that is abetting the illicit procurement network. This technique, while potentially very effective, also has costs and risks. It requires a complicit buyer based in the target territory and a way must still be found to get the goods out of the territory.

\textit{Buying, or Buying Into, a Supplier}

Another strategy that procurers have been known to pursue involves buying into commercial companies that are either manufacturers/suppliers of goods of interest in their own right, or due to the nature of their overt business are legitimate customers for such goods. In some cases such buying in has been conducted by individuals or commercial entities quite overtly and through normal commercial channels. Cases often involve producers of high technology goods that are in financial difficulty.

In other instances the act of buying into the target company was conducted through straightforward channels without the use of false identities or nationalities, but done in a discreet fashion that might escape attention by any parties with a nonproliferation interest. In some cases proliferators acquired a stake in target companies by means of a ‘silent partnership,’ whereby the proliferator had no official/legal stake in the target company, but behind the scenes and ‘off the books’ personal deals had been done with the target company owners/managers that gave the proliferator a de facto stake in, and ability to leverage/exploit, the target company.\footnote{47}


\footnote{46} For example, an Iranian procurer, Hossein Tanideh, introduced himself to clients as a ‘refinery manager’ while deceptively obtaining valves for Iran’s UN-proscribed heavy water reactor at Arak. Valves frequently have applications in petrochemical industries, and referring to himself in this fashion may have served to inspire confidence as a legitimate trading partner. See Daniel Salisbury and Ian J. Stewart, “Valves for Arak,” Proliferation Case Study Series, Project Alpha, August 22, 2014. <http://www.projectalpha.eu/proliferation/item/342-valves-for-arak>.


\footnote{47} An example of the ‘silent partnership’ approach has been given earlier, at footnote 40, concerning German company H & H Metalform’s relationship with Iraqi procurement figures in the 1980s. Purchasing a formal interest in companies in supplier countries was a method practiced by Iraq in the 1980s, with procurers acting for the Iraqi government involved in manufacturing companies in the UK and elsewhere: see Mark Fitzpatrick, ed., \textit{Nuclear Black Markets: Pakistan, A Q Khan and the Rise of Proliferation Networks – a Net Assessment} (London: International Institute for Strategic Studies, 2007), pp.45-46. More recently, in 2013, the \textit{Washington Post} suggested that Iranian entities may have attempted to purchase a bankrupt composite material component factory, located in Germany, in order to obtain the company’s specialised equipment and use it for nuclear- or missile-related purposes. See Michael Birnbaum and Joby Warrick, “A Mysterious Iranian-run Factory in Germany,” \textit{The Washington Post}, April 15, 2013, <https://www.washingtonpost.com/world/europe/a-mysterious-iranian-run-factory-in-germany/2013/04/15/92259d7a-a29f-11e2-82bc-511538ae90a4_story.html>. See also Cristina Rotaru, ‘The case of MCS Technologies – Did Iran Use a German Factory for Illicit Procurement?,” Project Alpha, King’s College London, August 19, 2015, <http://www.projectalpha.eu/proliferation/item/434-mcs-technologies-germany-iran>.
This strategy may be attractive as most countries do not have in place strong controls on foreign investment and company ownership. However, the cost of buying a controlling stake in a company is evidently still high.

Synergy of Methods for Approaching the Supplier

Interestingly, there are examples where all three mechanisms can be seen in cases of illicit procurement involving one company (subornation, deception and theft), such as the MKS case referred to above. This indicates that there can be numerous points of deception in a complex supply chain.

Evading the Authorities

The next step for the illicit procurer is to take measures to evade counter proliferation authorities. The majority of cases of illicit procurement appear to involve purchasing by conventional transactions from commercial suppliers, and subsequently export via normal commercial channels (whether this is performed immediately, or at a later date if goods have been purchased by a domestic customer acting for the illicit network). In such cases, the problem with regard to evading the authorities in the supplier country is threefold: firstly the export control authorities, secondly the border/Customs authorities at sea- and air ports and land border crossing points plus authorities acting within customs areas where trans-shipment can be carried out without the usual Customs controls, and thirdly those investigative agencies that are proactively seeking out intelligence on illicit procurement operations.

Firstly, illicit procurers must deal with the problem posed by export control authorities either by arranging for the goods to be exported without anyone contacting the export control authorities, or by having those authorities contacted and them granting an export license (or responding that no license is required). The procurers need to avoid a situation in which the supplier or any of the other parties to the deal (e.g. freight forwarders, financiers, shippers, insurers and so on) contacts the authorities because their suspicions have been raised or because of some automated alerting system.

Secondly, procurers must evade border controls and Customs. This primarily involves either having paperwork from export control authorities that grants an export license (or attests that no license is required), or by having the consignment appear to be one that doesn’t require any such permission. Alternatively the procurers might be able to arrange for border/Customs authorities at the relevant locations to be suborned into allowing the consignment to proceed.

Thirdly, the illicit procurers need to evade the attentions of those investigative agencies (whether they are intelligence services, law enforcement agencies, regulatory organisations including auditors, or other) that are specifically and proactively trying to discover illicit procurement, related activities and persons and organisations involved on an on-going basis. As a point of interest, it may be the case that for most of the time no-one really knows how effective illicit procurers’ evasion efforts are, until and unless some watershed event arises that reveals the historical activities of a particular programme in detail, such as the

48 Financial and operational drivers that incline illicit procurers towards working through normal commercial channels in order to transport goods are discussed in Justin V. Hastings, “The Geography of Nuclear Proliferation Networks,” Nonproliferation Review 19:3 (November 2012), pp. 429-450.

49 Such ‘customs areas’, surrounded by a ‘customs border,’ are usually designated within ordinary air- and sea ports, and at land border crossings, and allow easy transhipment of goods in transit to another country without the necessity of clearing customs. Free ports or free zones, sometimes termed bonded areas, may also have no customs controls for goods being transhipped, or have more relaxed customs regulations than normal.

coalition military campaign against Iraq in 1991 and subsequent UN inspection efforts.

**Dealing With Export Control Authorities**

Options for dealing with export control authorities vary. A key factor is whether or not the goods are of a type and specification which is listed under one of the control regimes (such as the NSG list) that are relevant in the country where the goods are being bought. If so, then there will be a legal obligation on suppliers to inform the export control authorities, and ask for an export license to be granted. Similarly, if the given end-destination is one that is subject to sanctions and embargoes then there may be a legal requirement to contact the authorities for export permission even if the goods are not on the usual control lists (in some cases certain sanctions regimes may simply ban all exports to that destination. Finally, in a particular country there may be obligations in some circumstances for those involved in an export deal to report the deal to the authorities even where the nature of the goods or the end-destination are not listed. In some countries with so-called ‘catch-all legislation’, a legal obligation may exist in any case where a party has reasonable suspicion that the goods will go to illicit use.

**Cases where the Authorities Are Contacted**

If the authorities are contacted the procurer will have to supply details to the supplier to pass on to the authorities, that will satisfy the scrutiny of those authorities. This presents a certain element of risk for the illicit procurer. The authorities may have information which will allow them to spot something untoward. For example, they may have access to intelligence information which gives identities or contact details for some illicit procurers, or may have information about particular requirements for proliferation programmes which dovetail with the goods being sought.  

The authorities may have greater ability to carry out probing due diligence checks than commercial companies, possibly including pre- and /or post-delivery verification visits to the claimed end-user. Furthermore, in some circumstances it may be possible to repeat post-delivery verification after the initial post-delivery check, which can be a means of preventing, or at least detecting, subsequent further export of the goods to another country. Post-delivery inspection can also help guard against the movement from a legitimate user to another, illegitimate, user in the same country. Another contingency is the diversion of goods in place, where they are used for legitimate purposes that can be declared to the supplier and that supplier’s government, but are at times used in the same location for illicit purposes.

In general government authorities in an exporting country may have greater abilities to carry out in-depth due diligence, possibly with the assistance of classified intelligence information. In some situations the authorities may be easier to deceive than an alert non-complicit supplier with a more detailed understanding of the market for their own goods, whereas in other cases the greater hurdle may be to deceive the authorities.  

In cases where the procurer has suborned the supplier, both parties can conspire together to produce a

---


submission to the authorities that is most likely to survive scrutiny.\textsuperscript{53}

The illicit procurer could contemplate attempting to suborn the export authorities. However, in general this is likely to be a difficult proposition, unless corruption is very widespread in the country concerned. Identifying which officials will be involved in the scrutiny of a particular export case may be challenging, and ensuring that the case is not reviewed by others is another problem. Some of those involved in reviewing license applications may have security clearances which allow them to see intelligence material and therefore should, in general, be individuals who are more difficult to suborn.\textsuperscript{54}

Cases Where Authorities Are Not Contacted Involving Listed Dual-Use Goods

If an illicit procurer has suborned a supplier the co-conspirators may decide not to contact the authorities, and attempt to export the goods anyway. This might involve using an anodyne description of the goods that made it appear that they were not relevant to export controls. There might be some residual risk that the goods would be stopped by Customs and questions asked regarding the details of the consignment.

However, if the in question goods were not of a type or specification that appeared in export control lists then, unless there was evidence that the supplier knew, or (in some jurisdictions) had reasonable grounds for suspicion, that the consignment was headed to a proliferator’s programme, it is unlikely, in the absence of some specific evidence, that it could be proven that the supplier had transgressed (unless they had contravened any relevant sanctions or embargoes).

Dealing With Border/Customs Authorities

In general, if the export licensing authorities have been contacted regarding a particular consignment, and have given approval for its export, then the border and/or Customs authorities at ports and borders will not present an obstacle. However, if goods are being exported without approval, a possible point of failure may occur when they pass through Customs and border checks. At this point an official (or automated risk management system) may hold up the shipment for further investigation.\textsuperscript{55}

Consideration might also be given to other methods of smuggling which avoid the goods concerned being moved through normal commercial channels, such as hand carrying of items on aircraft – a technique that has been used in the past.\textsuperscript{56} Other possibilities involve the use of private aircraft and the use of sailing boats.

\textsuperscript{53} A reported case where both the supplier and procurer conspired to submit false details to authorities occurred in 2015, when US authorities disrupted an alleged procurement ring involving a US manufacturer of electronic systems, Smart Power Systems, with an Iranian sister company, Faratel. The two companies allegedly conspired to procure electronic components for Iranian military or missile-related end-users. See Christopher Coughlin and Andrea Stricker, “Case Study: Skilled Procurement Ring Charged in Illegally Obtaining Goods for Iran,” Institute for Science and International Security, May 5, 2015, <http://www.isisnucleariran.org/assets/pdf/Skilled_Procurement_Ring_Faratel_5May2015.pdf>.

\textsuperscript{54} As an example of subornation amongst government figures and others of influence, a Philippines-based conspirator of an Iranian illicit procurer claimed to have the support of “politicians or bigtime [sic] businessmen” in Manila who purportedly helped smooth illicit transactions. See Daniel Salisbury, “Khaki-Yi, Project Alpha Case Study in Illicit Procurement,” Project Alpha, King’s College, 2013, <https://www.acss.info/proliferation/item/download/19_fce993c94c0bd060b52f205af729f6ff1>.

\textsuperscript{55} Events such as these, e.g. ‘Customs stops’, may be prompted by a number of things. There may be something about the consignment, the details provided, those handling it, and so on, that arouses suspicion. Alternatively, a consignment may be stopped without any suspicion having been aroused, simply as a part of ‘spot checks’. The task for the illicit procurer is to try to ensure that nothing about the consignment appears suspicious enough to warrant a stop. Providing the details of the goods, consignee, etc. appear benign, and none of the identities and contact details on the accompanying paperwork match with identities on any ‘watch-lists’ held by the border authorities, then in most cases there will be no reason to hold the consignment up.

\textsuperscript{56} In 2009, Iranian procurers reportedly had plans to send a shipment of gyroscopes and accelerometers to Iran’s missile programme by having a visiting Iranian government delegation carry them in travel bags on their return to Iran. See “Informing Beijing of Chinese Firm Limmt’s Continued Proliferation to Iranian Ballistic Missile Program (S),” Wikileaks, March 18, 2009, <https://wikileaks.org/plussd/cables/09STATE25689_a.html>.
Developing and Maintaining Assets and Infrastructure

Another important feature of illicit, nuclear related trade across the programmes mentioned above is the existence of transnational networks which, to a greater or lesser degree, share methods and tactics. The networks themselves appear to vary substantially in size, shape, and durability. While it is the A.Q. Khan proliferation ring that may spring to mind when thinking of networks, in reality most networks are likely much more transient and ad hoc in nature, and the degree to which individuals in the ‘downstream’ elements of the procurement chain (i.e. those closest to the supplier) may be fully witting to the real intended final destination and end-use may vary considerably.\(^{57}\)

To a greater or lesser extent, depending on the specifics of a particular procurement effort, there may be a need to develop assets and infrastructure for the network. These include ‘front companies’, commercial premises, warehouses, ‘safe houses’, communications equipment, and so on. Some networks may contain individuals, commercial entities and infrastructure that are significantly ‘tethered’ in countries that are opposed to the illicit procurement effort (or would be if aware of it) or neutral (and could possibly become hostile). To varying degrees, some procurement networks operate with assets ‘at risk’ in hostile or potentially hostile territory. This presents a potential vulnerability but such assets may often present the network with valuable capabilities (for example an apparently reputable company in the same country as significant potential supplier companies, may be able to make sales enquiries and purchase goods).

Other networks may be set up in a much more light-footed and less ‘forward-deployed’ fashion, foregoing some useful capabilities for a less vulnerable and often less expensive set-up.\(^{58}\) Illicit procurement can often be performed almost ‘from the bedroom’ these days. This is illustrated by cases of illicit procurers such as the Austrian Daniel Frosch, who operated from home, without warehouse or any significant overheads, and likely just a computer.\(^{59}\) At a minimum, an instance of illicit procurement is likely to require arrangements for a ‘front entity’ of some sort to be available that can be declared as the customer. This entity will need to appear be a credible customer with a legitimate use, at least when subject to whatever level of scrutiny is going to be forthcoming from the authorities.

The front entity might be a purely fictitious creation, whose name is simply given by the illicit buyer to the supplier along with a delivery address and contact details where the procurement network can take messages and pick up the goods. Alternatively the procurement network might create a real organisation, but one which does not actually carry out any real business in its declared line, and instead is used purely to enable illicit trade. Another option is to use a real entity carrying out legitimate activities but use it to enable illicit activity. Setting up and maintaining any of these arrangements in a way that passes scrutiny by any potentially hostile authorities, and meets all the requirements of the illicit procurement network (which may include being economically viable as well as successfully enabling illicit trade), requires certain skills and knowledge which go beyond regular legitimate commercial practice.\(^{60}\)

\(^{57}\) Some indication in the transient nature of procurement networks is of the sheer number of entities – some several hundred – that have been subject to designation by the US government and European Union for their involvement in illicit procurement. New procurers apparently emerge on a regular basis, and others cease activity for a variety of reasons, including due to law enforcement action.


\(^{60}\) Some indication of this is given by the case of Karl Lee (aka Li Fangwei), a China-based businessman who has been reportedly supplying Iran’s missile programme for the last decade, despite repeated efforts by US authorities to stop him. Lee’s survival suggests a certain level of savvy and adaptability. See Ian J. Stewart and Daniel B. Salisbury, “Wanted: Karl Lee,” The Diplomat, May 22, 2014, <http://thediplomat.com/2014/05/wanted-karl-lee/>.
At the other end of the spectrum, an illicit procurement network may do business in such a way that as well as a ‘front’ entity to pose as a legitimate customer, its operations involve a more extensive clandestine infrastructure, possibly involving setting up additional front organisations to act as the buyer or other intermediaries, some of which may be based in the same countries as the supplier entities are located in. Depending on the specific nature of the operation, there may be a need for provision of facilities such as safe houses, clandestine communications arrangements, falsified documents, special financial arrangements, alias identities for some individuals involved, transport and other logistics facilities under the control of the procurement network, and so on. Setting up and maintaining such a clandestine infrastructure while faced with the potential threat posed by hostile authorities requires a range of skills and resources that may be very challenging. More complex clandestine infrastructure for illicit procurement has often been set up and maintained by, or with the aid of, the proliferator state’s intelligence service.61

**Network Communication**

An important aspect of proliferation networks relates to communications. Communications are vital for such networks but are also a source of risk. Should authorities be able to intercept the network’s communication, the network’s operations would be compromised. The Snowden revelations may have helped networks develop communication methods that are less susceptible to intercept by authorities. However, even if so, proliferation networks must still communicate ‘in the clear’ with suppliers and authorities, leaving open an opportunity to gain insight into their activities. Great care and skill is therefore required in such networks if their communication is not to be compromised.

As in many other areas, there is a trade-off involved for networks that wish to practise more clandestine and secure communications, in terms of generally decreasing speed, increased expense, and increased man-hours required. There is also the possibility that sometimes the use of such techniques will not evade attention but will actually highlight that the network is engaged in illicit activity. Judgement of whether and when to use enhanced techniques or to stick more closely to normal commercially-confidential business practice may be a key skill for successful illicit procurement campaigns.62

**Use of Diplomatic Cover and Premises**

International diplomatic conventions furnish nation-states with the ability to overtly set up relatively secure facilities on the territory of any country with which they have diplomatic relations. The confines of an embassy are only relatively secure because of the common employment of local nationals in some roles and the high possibility that parts of an embassy building and grounds have been compromised by planted listening devices and the like. However within an embassy a capable nation can install secure meeting rooms and communications facilities that have a high degree of security.63 A diplomatic post thus furnishes a country with a multi-purpose facility which its nationals (and other guests) can overtly visit for all manner of potential purposes, and where confidential meetings can be conducted, records stored, and secure messages sent and received using encrypted communications. The frequent secure sending and receiving of encrypted communications via a range of telecommunications channels is routine, and of itself tells the host country

---

61 Iraq’s procurement activities under Saddam Hussein provide a clear case. As the CIA has noted, ‘the Iraqi Intelligence Service (IIS) and the Military Industrialization Commission (MIC), however, were directly responsible for skirting UN monitoring and importing prohibited items for Saddam.’ See “Comprehensive Report of the Special Advisor on Iraq’s WMD,” CIA, December 30, 2004, <https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/chap2.html>.

62 However, in practice considerations of the potential for personal profit-making may often be an important factor in determining the extent to which different methods are selected.

63 The procurement network of Karl Lee, a Chinese businessman who has purportedly supplied Iran’s ballistic missile programme with dual-use goods, has been facilitated by Iranian operatives working from the country’s embassy in Beijing. See for example, ‘Informing Beijing of Chinese Firm Limmt’s Continued Proliferation to Iranian Ballistic Missile Program (S),” March 18, 2009, <https://wikileaks.org/plusd/cables/09STATE25689_a.html>.
little of significance (although increased levels of message traffic on occasion can be of interest).  

Furthermore, the diplomatic immunity conferred upon those members of an embassy’s staff who are accredited diplomats recognised by the host country allows such personnel to carry out activities which if exposed would normally lead to criminal prosecution in the country concerned, but would only subject a diplomat to expulsion from the country and being made persona non grata.

A diplomatic post can thus provide a convenient and easily accessed base of operations for illicit procurement activity, and a useful meeting location and short-term support facility for visiting members of an illicit procurement network, or in some circumstances for network members permanently based in the country concerned.

One particular feature of international diplomatic conventions that is particularly interesting when examining illicit procurement is the diplomatic bag (aka diplomatic pouch) service operated by diplomatic posts. This allows posts to send and receive packages marked as diplomatic correspondence, sent between diplomatic posts of a particular country and their home government, which should not be opened by anyone other than that country’s authorised officials. Security of diplomatic pouches, and immunity from having their passage obstructed, is guaranteed under the Vienna Convention of 1961 and appears to be generally respected in most countries around the world. Given the wide parameters acceptable with regard to type of package/container, size and weight, many items that have been procured and taken to diplomatic premises can in principle be placed in a diplomatic pouch which is then sealed and sent out of the country. For example, it is reported that in the late 1980s Iraqi procurers obtained a sample of maraging steel from a black market supplier (actually a British national) while in France, and that the sample was taken by one of the procurement team to the Iraqi Embassy in Paris. It was then sent by diplomatic pouch to Germany,

---


67 The case of Karim Ali Sobhani, Iranian intelligence officer and procurer, is also worth noting. Sobhani was active in illicit procurement activities during the 1980s while serving under diplomatic cover in Germany. Indicted for export-related offences by the US, he was declared persona non grata by the German government. However he subsequently resumed procurement activities in Europe while acting under non-official cover, and during this time visited the Iranian Embassy in Bonn on business. See New York Times News Service, “US Fights Germans’ Aid to Iran,” Chicago Tribune, June 27, 1989.

68 Within reason, all manner of objects can be packaged and placed in a diplomatic ‘pouch,’ as the physical form of ‘pouches’ can vary considerably, and can range from a brief case, sack, crate or even potentially a shipping container. The Vienna Convention sets no limits on the physical size of a designated diplomatic pouch, nor its weight. Similarly, there is no generally agreed convention formally recognised by most nations regarding form, size or weight. In practice there have been occasions when a nation has challenged the validity of a particular diplomatic pouch on the grounds of size and weight, for example in 1984 the Swiss authorities challenged the Soviet Union’s attempt to have a 9 ton trailer truck regarded as a diplomatic pouch, and stated that they regarded 450 lbs. to be the maximum acceptable weight for a legitimate diplomatic pouch. However such opinions on reasonable size limits for diplomatic pouches are by no means generally accepted. See Charles Ashman and Pamela Trescott, Diplomatic Crime: Killings, Thefts, Rapes, Slavery & Other Outrageous Crimes (Washington DC: Acropolis Books Inc., 1987) and “Pouch Without a Home,” Time Magazine, July 30, 1984, <http://content.time.com/time/magazine/article/0,9171,926723,00.html>.

69 For a discussion of the obligations and immunities adherence to the Convention involves concerning diplomatic bags, see Michael Hardy, Modern Diplomatic Law (Manchester: Manchester University Press, 1968), pp. 39-40.
where it was taken to a commercial company for testing.\textsuperscript{70,71}

\textit{Protecting the Network: Secrecy, Security and Counter Intelligence}

A proliferation programme with an illicit procurement component is likely to be the target of intelligence-gathering efforts by a number of investigative agencies from a range of countries. This might be expected to cause some of those involved with illicit procurement to consider the risks they run in having their procurement network penetrated by one or more of these hostile agencies.\textsuperscript{72} Security measures might be taken such as ‘vetting’ those who will be involved in illicit procurement activity, to the extent possible, and restricting information according to ‘need-to-know’ principles. A proliferation programme might also consider carrying out some clandestine investigation of people within its procurement network or their key business contacts, where practicable. These activities might require significant effort if undertaken, however this would need to be set against consideration of the risks to the illicit procurement effort and the proliferation programme if the procurement network was penetrated, and its efforts impeded or sabotaged.

Another potential security activity is organising network activities so that individuals with access to sensitive information are less able to either deliberately betray the network on their own initiative, or be targeted by hostile intelligence/investigatory services. An example of this might be some situations involving technical experts from the proliferation programme who do not routinely travel abroad, but might sometimes be needed to accompany procurers who for a particular mission do not have sufficient technical expertise.\textsuperscript{73} In such cases specialists, particularly if they are traveling under their own names (which may often be more practical) and have become known overseas in the past (for example if they have studied abroad) may attract attention from hostile agencies.\textsuperscript{74} Sophisticated procurement networks may consider using measures to reduce the risks, such as placing their specialists under some form of counter-surveillance and monitoring open source and social media about the project and its staff.

\textit{Counter-Intelligence Activity}

If someone is trying to do the utmost to preserve the security of a an illicit nuclear programme and its procurement efforts then one important task is the collection, collation and analysis of information that provides indications to what counter-proliferation authorities know about that programme. Apart from material gained through intelligence sources and methods, information can come from a variety of more easily accessible sources, including court reports of prosecutions for export control violations, information provided to the defence in the course of a prosecution, press reporting of public statements by officials and politicians, open political debates (e.g. parliamentary proceedings) and from both informal diplomatic warnings and formal protests such as demarches to the proliferator government concerned.

There might also be the option to attempt to feed in misinformation to investigative agencies using any intelligence channels available. Effective deception operations of this sort might require a relatively high degree of skill from the agency performing them, but some of the countries who have engaged in nuclear proliferation in recent history have possessed foreign intelligence arms with a significant capability to

\textsuperscript{70}The use of the diplomatic pouch by Iraqi procurer Obeidi has been mentioned earlier. For the use of diplomatic pouches by Pakistan, see Gordon Correra, \textit{Shopping for Bombs} (Oxford: Oxford University Press, 2006), p. 22.

\textsuperscript{71}A further example of the use of the diplomatic pouch by proliferators is given in Armstrong and Trento, \textit{America and the Islamic Bomb} (Hanover: Steerforth Press, 2007), p. 68.

\textsuperscript{72}By 2003, the CIA had reportedly recruited three Swiss-based members of the A.Q. Khan network who provided highly-detailed knowledge of the network’s activity. See Catherine Collins and Douglas Frantz, \textit{Fallout: The True Story of the CIA’s Secret War on Nuclear Trafficking} (New York: Free Press, Simon & Schuster, 2011).

\textsuperscript{73}See Obeidi and Pitzer, \textit{The Bomb in My Basement} (New York: John Wiley & Sons, 2004).

\textsuperscript{74}For an account of travels by Iraqi technical specialists on illicit procurement missions to Europe in the 1980s, see Obeidi and Pitzer, \textit{The Bomb in My Basement} (New York: John Wiley & Sons, 2004).
conduct clandestine operations with considerable international reach.\textsuperscript{75}

**Points of Deception**

The previous sections have highlighted that for proliferation to occur, a point of deception must normally exist (except in a situation where the country from which the goods are supplied is uninterested in nonproliferation, at least where the particular country of destination is concerned, or is bereft of export controls). From the examination of proliferation techniques and proliferation networks above, it is apparent that points of deception could rest almost anywhere in the supply chain. For example, if the supplier has been co-opted into illicit procurement then the supplier would have to deceive the licensing and/or Customs authorities, and the primary point of deception in such a case could be considered to lie at the juncture between the complicit supplier and the authorities. In general, someone upstream of the point of deception would engage in the deception of parties downstream, be it to deceive the supplier, the supplier’s licensing authority, Customs, etc. The list of those who may be deceived is also not limited to supplier and government authorities: shippers, insurers and financiers could also have a role to play.\textsuperscript{76}

It was also suggested that several programs had utilised these techniques in support of their clandestine nuclear and missile programs. In this context, it is useful to briefly review the use of these techniques in the cases of certain nations. For this review, Pakistan, Iraq and Iran were selected. The reason for selecting these cases relates primarily to the substantial amount that is known about how the nuclear and missile programs of these countries have procured goods. Libya was discounted as it was the A.Q. Khan network rather than the Libyan government that had responsibility for procuring most of the items.

**Pakistan**

Pakistan’s nuclear program started in earnest in the early 1970s and accelerated after the Indian peaceful nuclear explosion in 1974. Pakistan turned to illicit procurement after its efforts to procure reprocessing capability from France were frustrated. In the 1970s, much of Pakistan’s illicit procurement was coordinated from diplomatic missions overseas. In particular, individuals based in Pakistan’s mission to Germany played a key role. By the late 1970s and 1980s, Pakistan relied on networks of complicit and ignorant European suppliers, often taking advantage of lax export controls and profit-motivated businessmen. Since the 1990s, the bulk of Pakistan’s illicit procurement seems to have been through entities in Pakistan acting as front companies.

Interestingly, there have been few known instances of Pakistan buying into overseas firms. However, Pakistan has utilised nearly every other procurement technique available.

**Iraq**

Iraq’s illicit procurement began after the destruction of the OSIRAK reactor in 1981. Saddam placed high importance on the country’s nuclear program, resulting in use of the entire state machinery to move it forward. For example, in the CIA’s comprehensive assessment of Iran which was conducted after the 2003 invasion and which drew upon Iraqi documents, it was noted that: \textsuperscript{77}

\textit{Saddam used the [Iraqi Intelligence Service] to undertake the most sensitive procurement}


missions. Consequently, the IIS facilitated the import of UN sanctioned and dual-use goods into Iraq through countries like Syria, Jordan, Belarus and Turkey. The IIS had representatives in most of Iraq's embassies in these foreign countries using a variety of official covers. One type of cover was the “commercial attaches” that were sent to make contacts with foreign businesses. The attaches set up front companies, facilitated the banking process and transfers of funds as determined, and approved by the senior officials within the Government.

The MFA played a critical role in facilitating Iraq’s procurement of military goods, dual-use goods pertaining to WMD, transporting cash and other valuable goods earned by illicit oil revenue, and forming and implementing a diplomatic strategy to end UN sanctions and the subsequent UN OFF program by nefarious means.

Saddam used the Ministry of Higher Education and Scientific Research (MHESR) through its universities and research programs to maintain, develop, and acquire expertise, to advance or preserve existent research projects and developments, and to procure goods prohibited by UN SC sanctions.

Iraq under Saddam successfully devised various methods to acquire and import items prohibited under UN sanctions. Numerous Iraqi and foreign trade intermediaries disguised illicit items, hid the identity of the end user, and/or changed the final destination of the commodity to get it to the region. For a cut of the profits, these trade intermediaries moved, and in many cases smuggled, the prohibited items through land, sea, and air entry points along the Iraqi border.

Iraq also made extensive use of the technique of buying out overseas manufacturers. The entities that Iraq targeted for takeover were often in financial difficulty.78

Iran

Iran’s nuclear program paused after the fall of the Shah but resumed during the Iran-Iraq war, during which Iran was approached by A.Q. Khan. Iran bought designs for Pakistan’s basic P-1 centrifuge and a limited number of parts, and later designs for the more advanced P-2 centrifuge. However, Iran did not procure wholesale the capability to enrich uranium as Libya did. Instead, Iran set about making and buying what was needed. Iranian illicit procurement has been largely commercial in nature, with Iranian nationals securing the support of intermediaries via financial inducement. Iran has also made extensive use of front companies.79

There are some signs that Iran has used diplomatic cover in pursuit of components and expertise. Iranian diplomatic officials in China have reportedly assisted procurement of missile components, although known cases are dated from more than five years ago.80 Officials from an Iranian state agency known as the President’s Technology Cooperation Office have also reportedly been involved in procurement of WMD-related expertise.81

78 For some insights into Iraq’s approach in the 1980s, see Obeidi and Pitzer, The Bomb in My Basement (New York: John Wiley & Sons, 2004).
81 An Iranian dissident group has alleged that the Technology Cooperation Office was responsible for recruiting a former Soviet nuclear weapons scientist who has reportedly provided nuclear weapon-related expertise to Iran. See “Exposing the Parchin
There are a few reported examples of Iran having bought out foreign manufacturers for the purposes of obtaining controlled technology. Examining these three cases highlights several trends. First, use of illicit procurement was generally similar in all three cases, albeit with some variations. Second, use of diplomatic premises appears to have declined (or has been detected less frequently). This may be due to proliferators judging that, given the amount of past reporting of activity by diplomatic staff, use of such personnel as procurement agents may simply attract the attention of national authorities. However this would not necessarily affect the utility of using diplomatic bag arrangements to get some goods, procured by other parties, out of the originating country. If the use of diplomatic bags has actually declined then the reasons for this are not clear. Additionally, the buying out of manufacturers also seems to have declined. Again, the reasons for this (if a genuine trend) are unclear.

**Points of Deception and Nonproliferation Controls**

This paper has examined illicit trade supplying dual-use goods to proliferators’ nuclear programmes and to some extent has considered such supply to associated missile delivery system programmes. The examination of this trade through the points of deception framework has highlighted several challenges to the effectiveness of nonproliferation controls, as well as some opportunities.

It is clear that illicit procurement techniques undermine the effectiveness of nuclear nonproliferation controls. Supply-side controls, generally aimed at controlling exports of relevant dual-use goods and, to a lesser but growing extent, broader aspects of strategic trade controls, have been expanded since the 1970s and have served to create increasing obstacles. However, through the use of increasingly indirect and deceptive methods, procurers have continued to acquire goods, albeit with increasing financial outlay required and delays incurred.

Situations in which a supplier or an element thereof is complicit, and an end user has provided credible false end use information, appear to be particularly difficult to thwart. There are certainly steps that states can take to reduce the likelihood of complicity. This includes awareness raising to remove ignorance and enforcement action to change cost/benefit calculus.

There are additional steps that companies could take to mitigate supply chain issues. For example, MKS Instruments Ltd., which was mentioned above, has implemented a “controlled delivery model” in which distributors are not used and all customers are subject to end use verification. In some sectors, this supply-chain model presents a credible opportunity to mitigate supply-chain risks. It should be recognised, however, that for most sectors such a model would not be suitable as it would substantially disrupt usual commercial practise.

However, use of similar models including end-use verification, whether carried out by the supplier company, the state of origin, or both, would appear to be a particularly valuable tool. It seems desirable that, as far as is feasible, similar practices are instituted internationally to cover the most critical industry sectors. It may be useful to identify where any arrangements are currently in place with regard to the various commercial sources of supply most directly relevant, starting with items identified in the Nuclear Suppliers Group (NSG) list of controlled dual-use goods.

---

82 For suggested definitions of strategic trade controls vis-a-vis strategic trade controls, and what these entail, see Catherine B. Dill and Ian J. Stewart, “Defining Effective Strategic Trade Controls at the National Level,” Strategic Trade Review 1:1 (Autumn 2015).

83 For further details regarding MKS’s approach, see Ian Stewart and John McGovern, “Beyond Compliance: Preventing the Diversion of Sensitive Vacuum Measuring Equipment – The “Controlled Delivery Model,” Project Alpha, King’s College London, September 2013.

84 The various known commercial suppliers for these goods were identified in “Commercial Producers of NSG Controlled
It is also apparent that national export controls cannot be expected to prevent shipment via diplomatic pouch, domestic sales of sensitive items, or foreign investment in domestic industry. In this context, the importance of other methods is key. Intelligence activities appear to present a particular opportunity to counter illicit procurement. Another area where it might be prudent to make more efforts relates to scrutiny of foreign investments in manufacturing firms.

This paper has focused on nuclear proliferation and has only briefly touched upon associated missile delivery systems. However the foregoing has given no reason to believe that the methods used to procure for such missile programmes are essentially different. While the specific problems involved in areas such as inventing plausible benign end uses to declare for goods being sought may differ, the essential problem appears to be the same. In addition, although this paper has not examined any instances of procurement for an illicit chemical or biological weapons programme, the techniques general necessity for the procurer to successfully establish at least one point of deception would appear to be applicable, even though the sheer scale and diversity of the chemical, biotechnology and related industries worldwide may offer more opportunities to hide illicit activity.

Conclusions

The growing scope and coverage of supply-side nonproliferation controls focused chiefly on strategic export controls, and to a broader extent strategic trade controls (such as controls on brokering in some countries’ legislation) has changed rather than prevented procurement for nuclear and missile programs. Several states have relied upon similar techniques over the course of the last four decades suggesting that current nonproliferation controls can be poorly suited to preventing such behaviour. Current controls rely heavily on export control regulations which can be difficult and resource-intensive to enforce.

The paper has presented a model – “points of deception” - through which such illicit trade can be understood. It is notable that according to information available through open sources proliferators have been reported to utilise nearly every technique that was identified through the model.

Examination of illicit trade through the model provides certain insights into what measures could be taken to disrupt proliferation networks. These include awareness raising and enforcement and the use of advanced supply-chain techniques to prevent complicity. It includes improving physical security and vetting in companies to prevent theft and insider threats.

The examination also highlighted the utility of scrutiny programs on inward investment to mitigate the risks of foreign buy-out, particularly for producers of sensitive goods that are in financial difficulty.

For certain risks that were identified through the application of the framework, such as the use of diplomatic bags to ship goods, there are no clear solutions. Instead, consideration should be given to how best to monitor domestic sales of proliferation-sensitive technologies.

This paper has examined a wide range of techniques and activities that fall within the tradecraft of illicit procurers. Although the sophistication, complexity, degree of direction and centralised organisation used in illicit procurement activities can vary greatly, in general in a particular procurement attempt an individual procurer or a wider network will have to successfully manage at least one ‘point of deception’ and may draw upon a range of other particular skills practised whilst carrying out procurement for ultimately clandestine means.

Illicit procurement can thus be viewed in part as a contest between the due diligence efforts of commercial suppliers and governments opposing proliferation together with those government’s counter-proliferation intelligence activities on one side, and on the other side the procurers’ ability to deceive, suborn, manipulate and generally manage the clandestine elements of their business, combined with proliferator government’s counterintelligence and security. This may be a useful viewpoint to take when devising or scrutinising nonproliferation controls, measures and postures, where some degree of war gaming or ‘red teaming’ the countermeasures that proliferators may use may be helpful to ensure that counter-procurement is made as effective as possible.

The use of illicit procurement techniques has been endemic since the 1970s. There are few reasons to suspect that use of the practices will end any time soon. Nonproliferation controls and efforts to prevent illicit trade can only slow down or frustrate illicit procurement. Ultimately, therefore, the international community must also look to other solutions in order to prevent proliferation. To that end, it will remain important to work continuously to ensure to that illicit procurement is countered as effectively as possible in order to buy time for other solutions to be developed.