Exploring the Use of 'Third Countries' in Proliferation Networks: the case of Malaysia

Dr. Daniel Salisbury, Centre for Science ad Security Studies, King's College London

Abstract: 'Third countries' are frequently exploited by those involved in networks to transfer proliferation-sensitive technologies, allowing procurement agents to obscure the end user or vendor located in the proliferating state, and to deceive industry, export licensing officials and intelligence services. While 'third countries' frequently feature in illicit transactions, the academic literature exploring the roles played by entities in these jurisdictions is limited. Building on the sanctions busting literature, this paper proposes a loose typology considering the ways in which third countries can be exploited by proliferation networks. The typology is illustrated using three cases involving entities based in Malaysia – AQ Khan's nuclear black market network, and Iran and North Korea's efforts to procure and market WMD-related and military goods. These cases are used to generate insights into proliferators' selection of 'third country' hubs. The paper argues that while exploitation of third countries by proliferation networks is a similar, but distinct phenomenon to trade-based sanctions busting, hubs of both activities share characteristics. Furthermore, the paper argues that other factors beyond the lax regulatory environment,

such as level of development, and personal connections, are often as important in driving the decisions of proliferation networks. The paper concludes with implications for nonproliferation policy.

Keywords: proliferation; arms embargoes; sanctions; illicit networks; Malaysia;

‘Third countries’ are frequently exploited by those involved in networks to transfer proliferation-sensitive technologies. This allows procurement agents to obscure the end user or vendor located in the proliferating state, and to avoid arousing suspicions of industry, export licensing officials and intelligence services. While ‘third countries’ have frequently featured in illicit transactions, the academic literature exploring the roles played by entities in these jurisdictions is limited. This paper uses an in-depth case study of Malaysia, a country having frequently played a role in these networks, to provide insights into ‘third country’ selection by procurement agents or arms traffickers. Rather than seeking to single out Malaysia, the paper uses the country –one of a number that have prominently played a ‘third country’ role in proliferation networks– to explore how these

countries are used by these networks, and the behavior of individuals and entities of which they are composed.

Building on the literature on economic sanctions busting, the paper presents a loose typology of the ways these networks use third countries, and the illustrates its applicability using three detailed case studies involving Malaysia-based entities: AQ Khan's nuclear black market network, and Iran and North Korea's efforts to procure and market WMD-related and military goods. In doing so, the paper considers what factors are involved in how proliferators select 'third country' hubs. The conventional wisdom suggests that Malaysia and other jurisdictions such as the UAE have featured prominently in these networks because of weak export controls, regulation and oversight. The paper compares proliferation networks' exploitation of third country hubs to Early's discussion of their use in trade-based sanctions busting.[1] It is argued that while distinct phenomena –notably trade-based sanctions busting focuses on volume of trade, while small, high-value transactions can make a big difference in proliferation networks– third country hubs in proliferation networks share some characteristics as hubs of trade-based sanctions busting. The cases explored in the paper also suggest that factors beyond the lax regulatory environment, such

[1] Bryan Early, *Busted Sanctions: Explaining Why Economic Sanctions Fail* (CA, US: Stanford University Press, 2015)

as the level of development, and personal connections, are often as important in driving the decisions of proliferation networks. The paper concludes by considering implications for nonproliferation policy.

1. Nonproliferation, Strategic Trade Controls and 'Third Countries'

Throughout the latter half of the twentieth century efforts have increasingly been made to prevent the proliferation of WMD – nuclear, chemical and biological weapons – and their means of delivery. As these efforts have seen a reduced number of governments willing to provide WMD-related technologies to other states, proliferators have increasingly turned to the international marketplace to obtain technology for their weapons programs. As the main supplier states have put in place export control systems in order to minimize the risk of diversion of exports to WMD programs, those seeking to procure WMD-related technologies have increasingly used illicit procurement networks and techniques to obtain controlled technologies.

Recent nuclear and missile proliferation cases – Iran and North Korea – have seen multilateral sanctions imposed against them by the UN Security Council, as well as unilateral sanctions imposed by various states. These complex sanctions regimes have included technology and arms embargos, travel-bans and asset freezes imposed on those directly associated with the weapons programs. The most recent North Korea resolutions have also imposed sanctions on sectors of the North Korean economy.

The rationale behind these technology-based sanctions on nuclear and missile programs –so called 'supply-side' measures– has been to prevent Iran and North Korea from obtaining requisite technologies, to slow the programs' development and to raise their costs. Under UN Security Council resolution (UNSCR) 1540 (2004) countries have been legally mandated to put in place export controls and other systems, in theory allowing them to implement sanctions, although UNSCR 1540 implementation has been very patchy in practice.

Economic sanctions more broadly –including the recent sectoral elements of UN North Korea sanctions– have been intended to affect the 'demand-side', pressuring Iran and North Korea to halt their pursuit of nuclear technologies. The UN arms embargoes have also

sought to affect these countries' will and ability to pursue nuclear weapons; arms sales have functioned to bolster ideological and political connections with allies, and in the case of North Korea, raise hard currency for its nuclear program.

To circumvent export controls and breach supply-side controls, procurement agents working for Iran and North Korea have employed techniques to deceive intelligence services, export controllers, customs officials, and industry compliance officers that are seeking to prevent exports to WMD programs. They include, but are not limited to, use of front companies, falsifying documentation, and concealing or mislabeling shipments. To breach the UN arms embargo, North Korea has also used front companies to market its arms. While many of these techniques remain unchanged since the 1970s, observers have suggested an increasing sophistication over time as procurement networks adapt to expanding measures to prevent proliferation.[2]

One of the techniques most frequently used by proliferators is placing procurement agents or brokers, or routing shipments, through third countries. The term 'third countries' or

[2] For example, a 2017 UN report noted North Korean efforts to evade sanctions of 'increasing in scale, scope and sophistication'. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017.

'third party state' is used in the literature on economic sanctions to describe players that are not the sanctions 'sender' or the sanctioned or 'target' state.[3] As used in this paper, the term has a similar but distinct meaning. Because some of the cases involve UN sanctions (universal and legally binding on all countries, which in theory means there is no 'third party') the term is used to describe countries utilized in transactions which are not the origin or destination of the goods being transferred. Other terms have been used in this manner, including hubs for 'transshipment' or, in cases of procurement, 'diversion' (where goods are diverted from their intended destination) and 'turntables' (where goods are imported and immediately turned-around and re-exported).[4]

While the use of third countries for deception purposes has frequently been used in WMD and military goods proliferation networks, there has been little effort to conceptualize the role played by these jurisdictions in the scholarly or policy literatures. Explanations have tended to focus on third countries being selected on the basis of weak export controls and

[3] 'Sender' and 'target' state used in Hufbauer et al., *Economic Sanctions Reconsidered 3rd Ed.* (Washington DC, US: Peterson Institute for International Economics, 2007) p.2; Early, *Busted Sanctions*, p.18.
[4] See for example 'Transshipment and Diversion: Are U.S. Trading partners Doing Enough to Prevent the Spread of Dangerous Technologies?', Hearing before the Subcommittee on Terrorism, Nonproliferation and Trade of the Committee on Foreign Affairs, House of Representatives, 111th Congress, 2nd Session, 22 July 2010, available at: https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg57609/html/CHRG-111hhrg57609.htm) accessed 17 May 2018; David Albright, Andrea Stricker and Houston Wood, 'Future World of Illicit Nuclear Trade: Mitigating the Threat', ISIS Report, 29 July 2013, available at: (http://isis-online.org/uploads/isis-reports/documents/Full_Report_DTRA-PASCC_29July2013-FINAL.pdf) accessed 17 May 2018.

enforcement. More nuanced conceptual thinking on this topic could have great value for our understanding of proliferation networks, and for developing proactive policies to counter them.

The Proliferation Networks and Sanctions Busting Literature

The existing scholarship largely falls into two different areas: Literature on the role of third country hubs in networks trafficking military and WMD technology has been fairly limited. There remains scope to further our understanding of the role of third countries by building on a second area of literature which is more developed: that exploring the role of third countries in economic sanctions busting.

References to 'third countries' in the proliferation network literature –that focused on the transfer of technology, often in breach of export controls or sanctions– are generally cursory and made in passing.[5] The literature on proliferation networks has largely focused

[5] See for example Chaim Braun and Christopher F. Chyba, 'Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime', *International Security*, 29:2 (Fall 2004), p.15; David Albright, Paul Brannan and Andrea Scheel Stricker, 'Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan', *Washington Quarterly*, 33:2 (2010), p.89.

on the state-level, with states forming the nodes: both suppliers and recipients.[6] More recently, some work has started to address what could be described as the 'transactional level', focusing on the role of, and interactions between, organizations, companies, and individuals.[7]

This work has sought to consider why elements of the private sector –individuals and companies– become involved in WMD-related illicit trade, providing a frameworks through which key motivations of profit, political and ideological interests can be considered.[8] However, while it is the private sector which largely provides the technology to proliferation networks, often the middlemen who broker these transactions, alongside the needs of these procurement networks, are ultimately driven by the state programs they supply. These 'witting' aspects of proliferation networks, especially the aspects based in third countries, have yet been fully explored in the proliferation network literature.[9]

[6] Alexander Montgomery, 'Ringing in Proliferation: How to Dismantle an Atomic Bomb Network', *International Security* 30:2 (Fall 2005), pp.172-3.
[7] Daniel Salisbury, 'Why do Entities Get Involved in Proliferation? Exploring the Criminology of Illicit WMD-related Trade', *Nonproliferation Review*, 24:3-4 (2017), pp.297-314; Aaron Arnold, 'A Resilience Framework for Understanding Illicit Nuclear Procurement Networks', *Strategic Trade Review*, 3:4 (Spring 2017), pp.3-23; Glenn Anderson, 'Points of Deception: Exploring How Proliferators Evade Controls to Obtain Dual-Use Goods', *Strategic Trade Review*, 2:2 (2016), pp.4-24.
[8] Salisbury, 'Why do Entities Get Involved in Proliferation?'
[9] For discussion of 'witting actors' – those aware their goods are destined for a WMD program – and 'unwitting actors' – those that are not – see Ian J. Stewart and Daniel Salisbury, 'Non-State Actors as Proliferators: Preventing their Involvement', *Strategic Trade Review*, 2:3 (2016), pp. 5-26.

Hastings provides the most developed conceptual treatment of third countries, taking a geographical approach to the Khan network, where nodes are 'people or organizations anchored in a specific piece of territory'.[10] He argues that networks without state prerogatives or resources –such as state-owned or military transportation, or embassies– must 'set up support structures that depend on advantageous economic, political, and social characteristics of their host countries'.[11] Considering Khan's efforts to supply Libya, Hastings focuses on Dubai as a key third country hub, as well as briefly considering the manufacturing operations in Malaysia, providing insights into selection of these hubs. Dubai's 'political and economic environment', lax regulations on setting up companies, place in global transportation infrastructure, high proportion of international residents, and lack of government oversight; and Malaysia's technological sophistication, lax regulation, and Khan's associate's existing social network are all cited by Hastings as factors.[12]

Hastings valuable work is not without limitation, essentially drawing its insights from three interlinked networks –all involving AQ Khan and some other common actors. The Khan

[10] Justin V. Hastings, 'The Geography of Nuclear Proliferation Networks: the Khan Network', *Nonproliferation Review*, 19:3 (2012), p.431.
[11] Ibid.
[12] Ibid., p.440.

network, arguably the most well-known and damaging illicit non-state supplier network in history, is clearly an anomaly, and possibly an anachronism. As Lieggi has noted, while Hastings portrays lack of state resources as a limitation, in recent years networks have moved from reliance upon state resources to take 'greater advantage of the globalized trade system', especially through benefitting from 'the virtual anonymity that can come with the use of major transshipment hubs and manufacturing locations'.[13]

The scholarship on economic sanctions busting, generally more developed than that on technology embargoes, has considered the role of third countries in undermining sanctions, but has not been consulted in relation to proliferation networks. The term 'black knights' was coined to describe 'powerful or wealthy countries' that provide support to undermine the effects of economic sanctions.[14] More recently, Early has drawn distinction between politically driven 'aid-based' and opportunistic profit-driven 'trade-based' sanctions busting, his work providing arguably the most nuanced treatment of sanctions busting to date. Early's concept of trade-based sanctions busting involves the development of 'alternative trading relationships' driven by profit-seeking private sector actors.[15] This is

[13] Stephanie Lieggi, 'Correspondence: Technology, not Geography, Drives Current Nuclear Trafficking Decision Making', *Nonproliferation Review*, 20:1 (2013) p.10.
[14] Hufbauer et al., *Economic Sanctions Reconsidered*, p.8.
[15] Early, *Busted Sanctions*, pp.18-19.

more relevant to considering proliferation networks than 'aid-based' sanction busting, which –driven and managed by governments– has more similarity with the state-to-state proliferation-related transfers.[16] Early's focus on economic sanctions necessarily means that his work concerns third party spoiling sanctions through making up declining trade with large volumes of business transactions. Focus on volume, or including proliferation-related alongside economic sanctions busting, is seen frequently in the literature.[17] While there are some similarities in the trade-based sanctions busting he has conceptualized –notably that goods tend to be sourced from the private sector and profit constituting the driver in some cases– the behavior of proliferation networks, in which small numbers of specialized transfers can make a big difference, is a different phenomenon worthy of similar nuanced treatment.

In sum, the nascent conceptual literature on proliferation networks has only considered third countries in passing, while that on sanctions busting largely considers a similar but

[16] 'Aid-based' sanctions busting is largely directed by governments, support could include transfers of 'developmental assistance, concessional loans or trade subsidies, grants, or military assistance'. Early, *Busted Sanctions*, pp.18-19. State authorized transfers undertaken using state prerogatives and resources are more likely, as Hastings notes, to avoid use of commercial third country hubs. Hastings, 'The Geography of Nuclear Proliferation Networks', p.431.

[17] For example, on Dubai, see Early, *Busted Sanctions*, pp.88-158; R.T. Naylor, *Patriots and Profiteers: Economic Warfare, Embargo Busting, and State-Sponsored Crime* (US: McGill-Queen's University Press, 2008); And on other cases see Peter Andreas, 'Criminalizing Consequences of Sanctions: Embargo Busting and Its Legacy', *International Studies Quarterly*, 49 (2005), pp.335-360

separate phenomenon. Discussion has failed to systematically consider the roles that these jurisdictions can play, and what factors results in their selection by proliferation networks. This paper uses a number of in-depth case studies in a single country– Malaysia—to consider questions specific to the role of third countries.[18] The Malaysian case presents a valuable opportunity for inquiry. The state has had no interest in developing WMD, and has a fairly small-scale but expanding defence industrial base. However, the country has seen significant proliferation-related activity over the past two decades through the Khan network, and Iranian and North Korean illicit trade, with many details about these activities in the public domain. Cases considered below include transfer of nuclear and missile technologies, as well as military goods and US origin technologies covered by the Iranian embargo. Emphasis has been placed on extracting data relating to individuals' decision making – for example through emails quoted in court documents—when available. In some of the Iranian cases involving goods covered by the US embargo, the goods themselves are fairly benign.[19] While the application of export controls can be politically and ethically contentious, this paper avoids discussion of these questions, focusing on the behavior and decisions of the networks. The significant data surrounding the cases allows for extraction

[18] This contrasts with Hastings's passing consideration of multiple hubs in the single, but interconnected, in the Khan case. Hastings, 'The Geography of Nuclear Proliferation Networks'.
[19] For example the Iranian cases involve transfers of an 'emergency floatation system'.

of data points directly relating to decision making by individuals involved in these networks, yielding fresh insights.

2. Third Countries in Proliferation Networks: Roles and Rationales

Given the paucity of existing conceptual scholarship on proliferation networks, this section presents a loose typology of the roles that third countries can play. Entities based in third countries can play three main roles in proliferation networks (Figure 1). This typology encompasses the vast majority of scenarios, and with the latter two roles –transshipment and brokering– being much more commonly seen than the manufacturing role.[20] Each of these roles will be illustrated using a Malaysia-related case study in the subsequent three sections.

Figure 1: Typology of Third Country Roles

[20] This is a more unusual phenomenon seen in the Khan network, for example: in Malaysia (explored below); and in the Turkish 'mini-hub', where importing parts from Europe were assembled into centrifuge motors and frequency converters. See International Institute for Strategic Studies, *Nuclear Black Markets: Pakistan, A.Q. Khan and the rise of proliferation networks: A net assessment* (London, UK: Routledge, 2007), p.81. Others have noted the potential for such a role, for example through manufacturing operations in 'free zones'. See Andrea Viski and Quentin Michel, 'Free Trade Zones and Strategic Trade Controls', *Strategic Trade Review*, 2:3 (2016), p.28.

Third Country Role	Definition	Third Country Footprint
Manufacturing	Facility used to work on imported technology, before re-export to program of concern	Medium to large
Transshipment or re-export[21]	Entity (individual or front company) used to import and re-export technologies to program of concern	Small to medium
Brokering (Marketing, sales or procurement)	Entity (individual or front company) used to broker deals involving technologies (technology does not necessarily enter the jurisdiction's customs area, or use its logistical hubs)	

[21] Transshipment occurs when goods do not enter the third country's customs area (for example, being moved from ship-to-ship at a port, or briefly warehoused and repacked at a Free Trade Zone (FTZ) taking advantage of the definition of transshipment in the third country's relevant legislation, typically for lesser licensing requirements). In re-export goods enter and exit the jurisdiction's customs area.

In presenting this typology, three caveats are stated: First, the typology largely refers to those that knowingly decide to utilize third countries in proliferation networks, and are 'witting' actors – those that understand that the goods are destined for a WMD program.[22] Second, the typology above does not include 'transit' – this is where goods might pass through the country's ports, without being off-loaded from the ship. This is because, rather than being indicative of the country being utilized in a proliferation network, cases where goods have transited a port tell us more about global logistical routes and transportation networks, and cases where shipments are seized whilst in transit tell us more about interdiction or enforcement action.[23] Third, the typology focuses on activities involving the movement (or planned movement) of goods, rather than also considering enabling functions such as financing or transportation.

The three third country roles set out have different 'footprints'– in spatial, social, legal and bureaucratic terms. The footprint is seen in a physical sense– manufacturing requiring a factory or similar facility; transshipment requiring a basic office set up, and possibly some kind of warehouse for larger items; and marketing or brokering requiring little more than a

[22] For a discussion of 'witting' and 'unwitting actors' see Stewart and Salisbury, 'Non-State Actors as Proliferators'.
[23] Imprecise reporting can make it difficult to make the distinction between transshipment and transit.

phone or internet connection.[24] In this context, footprint is also used to encompass often observable legal, bureaucratic and social, impact of these activities. A large factory or warehouse involved in a proliferation network could provide significant physical evidence of a network's activity. However, it also requires satisfying (or avoiding) significant legal and bureaucratic processes –everything from insuring imports and exports clear customs, employing and managing skilled labor from the local community or sourced from other countries, acquiring and maintaining manufacturing equipment, to paying corporate taxes.

A significant legal dimension relates to whether the actor decides to legally register a company in the third country to undertake its activities, or whether the illusion of a company is used. Creating this illusion could involve using a letterhead or a website. Both pathways create challenges and opportunities. The barriers to establishing a legal entity vary between jurisdictions. The legal registration may satisfy those conducting in-depth due-diligence, but could also involve more information on the organization being placed into the public domain of benefit to investigators.

[24] This article has adapted the term 'footprint' from the business literature, where it usually refers to physical space. See Jonathan Law ed. *A Dictionary of Business and Management 6th Ed.* (UK: OUP, 2016)

On the other end of the spectrum, the footprint of an individual operating as an arms broker could be minimal: operating alone, conducting meetings in hotel bars, carrying just a laptop and a phone. Individuals could, and frequently do, broker deals involving goods being shipped between two separate jurisdictions, with goods never passing or being transshipped through the country in which they are located. Footprint, as used here, does not necessarily imply the ability of the third country government or others to detect the proliferation-related activity. This would depend on the network's ability to hide its activities, and operational security.[25]

The use of third countries could in theory be avoided in all three of these transactions. Goods could in theory be procured directly from a supplier by the country hosting the WMD or military program, without need for transshipment or a broker located in a third country;[26] the function fulfilled by a third country factory could potentially be replicated in the destination, or more likely in the advanced supplier economy. However, the main rationale for the use of individuals or entities based in third countries is to *deceive*– to hide

[25] For example, in the SCOPE case explored below, the number of people with full knowledge of the end use of the goods the factory was producing was heavily limited. See Royal Malaysia Police, 'Press Release By Inspector-General of Police in Relation to Investigation on the Alleged Production of Components for Libya's Uranium Centrifuge Programme', February 2004, available at (http://isis-online.org/uploads/iaea-reports/documents/Malaysian_Police_Report.pdf) accessed 17 May 2018.
[26] See for example networks with state resources or prerogatives in Hastings, 'The Geography of Nuclear Proliferation Networks'.

the ultimate end-user of goods, connections to a sanctioned country or program, or in the case of the factory to prevent the need to procure finished goods with clear WMD application.[27] This avoids raising concern amongst industry and governments that would be triggered by direct approaches from, or attempts to license exports to, Iranian or North Korea-based companies. In doing so, the use of a third country adds a layer of deception by means of exploiting what is a normal characteristic of most international supply chains.

When it comes to the selection of specific hubs, the literature on criminal networks has coined the term 'jurisdictional arbitrage' to refer to transnational criminal groups efforts to 'exploit the differences in national laws and regulations'.[28] Countries which offer an environment with limited business regulation, limited enforcement activity and related oversight – with regard to export controls and in other respects– would clearly be advantageous to those seeking to avoid detection and disruption of their activities. Lack of political commitment on the behalf of the host government to the implementation of sanctions or export controls and a significant diaspora business community of the sanctioned country could also be advantageous.

[27] Anderson only alludes in passing to the use of third or 'intermediary' countries as 'deception points'. See Anderson, 'Points of Deception', p.8.
[28] Phil Williams, 'Transnational Criminal Networks', in John Arquilla and David Ronfeldt (eds.), Networks and Netwars (Santa Monica, US: RAND, 2001) p.71.

In the geography of illicit networks, distinction has been drawn between terrorist 'havens' offering lawlessness, and criminal 'hubs' providing some 'baseline level of infrastructure and services'.[29] The manufacturing and transshipment or re-export operations in the typology would clearly benefit most from those features of 'hubs': access to commercial transportation routes, secure warehousing, and in the case of a factory uninterrupted supplies of water and electricity, and access to skilled labor. The solo arms broker example would not necessarily require these features as urgently, although true 'lawlessness' would not be beneficial. The necessity of these 'hub' attributes is both to allow the basic functions of a factory, or warehousing, but also because requests for quotations for highly-advanced dual-use technologies originating in countries without a sufficiently developed industrial sector are likely to raise alarm.

The subsequent three sections present detailed case studies which illustrate these three types of third country roles. The cases are designed both to showcase the applicability of the typology, and to consider why the proliferators in those cases chose particular third

[29] Patrick Radden Keefe, 'The Geography of Badness', in Michael Miklaucic and Jacqueline Brewer (eds.), Convergence: Illicit Networks and National Security in the Age of Globalization (Washington DC, US: NDU Press, 2013), p.100.

country hubs. The cases are followed by a section which seeks to draw broader conclusions about the choice of Malaysia and the behavior of proliferation networks, before considering recommendations for policy.

3. Khan, SCOPE and Malaysia

In the early 2000s the scale of the proliferation activities of Pakistani nuclear weapons scientist AQ Khan started to become clear, although the full story regarding the Pakistani state's knowledge of his activities remains unresolved. Drawing on many of the contacts Khan had established in procurement for Pakistan's centrifuge enrichment program, Khan went on to coordinate the supply of centrifuge and other technologies to Iran, North Korea and Libya. The 'Libya deal', struck in 1997, involved the supply of a full gas centrifuge plant.[30] Fulfilling such a large order would require a more extensive manufacturing capability than previous deals which mostly relied on surplus goods from Pakistan's program.

[30] David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (US: Free Press, 2010) p.120.

Malaysia was selected by Khan's operation to host a significant manufacturing effort. Scomi Precision Engineering Sdn Bhd[31] (SCOPE) was used to manufacture centrifuge components. Four shipments were made of these components to Libya. The final of these shipments, which included 25,000 centrifuge parts – labelled 'agricultural machinery' in SCOPE marked crates – was shipped from Malaysia on a local ship in August 2003.[32] The shipment was warehoused in Dubai for 48 hours before being transferred on to the *BBC China*, which was interdicted in Italy on route to Tripoli.[33] This first case considers Khan's manufacturing operation in Malaysia and the rationales for the establishing operations in this jurisdiction.

The Libya deal was on a scale that hadn't been dealt with by the network before. It would eventually involve the transfer of 10,000 P-2 centrifuges – each including around 100 parts and components – meaning the production or procurement of around 1million parts.[34] The clear scrutiny any effort to locate new manufacturing operations in Pakistan or then sanctioned Libya would garner led Khan and BSA Tahir – a key figure in Khan's network –

[31] 'Sdn Bhd' indicates that the organization is a private limited company in Malaysia.
[32] Douglas Frantz and Catherine Collins, *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets...And How We Could Have Stopped Him* (NY, USA: Twelve, 2007), p.299.
[33] Ibid.
[34] The initial deal was for 5,000 centrifuges, but later expanded to 10,000. Albright, *Peddling Peril*, p.122; For 1 million figure see p.130.

to consider other options.[35] The most complex centrifuge parts were manufactured in the a factory in Switzerland owned by long-time collaborators, the Tinner family, while production of less complicated parts was outsourced to other 'third countries' – Malaysia, alongside South Africa, Turkey and others.

Accounts of the decision to establish operations in Malaysia suggest that several alternatives were considered. Originally, Dubai had been considered as an option– Urs Tinner had sought to establish a factory there but was unable to find a sufficient local skilled work force, and worried that work permit applications could stimulate government interest.[36] Second, Turkey was considered, but again the lack of skilled labor proved to be a problem.[37] A third location, South Africa, was also considered. South Africa had hosted a nuclear weapons program which was dismantled in the early 1990s, meaning labor shortages were less likely to be an issue. However, South Africa's history as a proliferator meant that governments may be wary about shipments of goods such as maraging steel to the country.[38]

[35] Frantz and Collins, *The Nuclear Jihadist*, p.235.
[36] Ibid., p.241.
[37] Ibid.
[38] Ibid., p.261.

Malaysia was first flagged as a further option by BSA Tahir in mid-2001, with the option explored further in the autumn.[39] Tahir, a Sri Lankan businessman ran the Dubai hub, and had rapidly become Khan's right-hand man.[40] Tahir had several personal and professional links with Malaysia. In June 1998 he had married a Malaysian woman – Nazimeh Syed Majid, daughter of a prominent Malaysian diplomat. Khan, alongside other network members, attended the wedding just months after Pakistan's first nuclear test.[41] Tahir's marriage meant he was eligible for permanent residency in Malaysia, although he generally spent most of his time in Dubai, as the Police report noted, only returning to Malaysia 'once in a while, to visit his wife's family or look for business opportunities'.[42] However, by 2000 Tahir owned an expensive building in Kuala Lumpur, and other businesses.[43]

Tahir 'mixed with Malaysia's elite' and grew close to Kamaluddin Abdullah, the son of Abdullah Ahmad Badawi.[44] Badawi was a long-time Malaysian MP, and would become Deputy Prime Minister in 1999, and Prime Minister in 2003. Kamaluddin appointed Tahir a Director of his privately held investment company, Kaspadu, which controlled Scomi

[39] Ibid., pp.261, 272.
[40] Royal Malaysia Police, 'Press Release by Inspector-General of Police'.
[41] Albright, *Peddling Peril*, p.134.
[42] Royal Malaysia Police, 'Press Release by Inspector-General of Police'.
[43] Frantz and Collins, *The Nuclear Jihadist*, p.261.
[44] Albright, *Peddling Peril*, p.134.

Group. Tahir's wife was also an investor in Kaspadu, and served on its board after Tahir.[45] While clear high-level connections to the Malaysian establishment, there is no evidence that Kamaluddin was aware of the nuclear dimensions of Tahir's activities.[46]

The decision to move operations to Malaysia was allegedly precipitated by a break-in at one of the network's Dubai warehouses.[47] Scomi Group signed a two-year $3.43mil contract in December 2001, and an existing company was acquired to handle the contract and renamed SCOPE.[48] Urs Tinner – by this point working as a CIA informant – moved to Malaysia to work as a consultant and help establish operations.[49]

An existing factory at Shah Alam outside of Kuala Lumpur – now owned by SCOPE – was refitted and would host 30 workers. Its capability was upgraded from producing car parts and industrial tubing to centrifuge components.[50] The upgrade, and the factory's new

[45] Gordon Correra, *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network* (Oxford, UK: OUP, 2006), p.113.
[46] Collins and Frantz, *The Nuclear Jihadist*, p.109.
[47] Ibid., p.46.
[48] Albright, *Peddling Peril*, p.135. According to the Malaysian company registry the company became SCOPE from 'Prisma Wibawa Sdn Bhd' in December 2001.
[49] Open sources do not suggest that the network's move was precipitated by the CIA. Albright, *Peddling Peril*, p.135.
[50] Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (NY, US: Free Press, 2011), p.47.

operations, required the import of equipment and materials. Aerospace grade aluminum was provided to SCOPE by Bikar Metal Asia in Singapore, sourced from entities in four other countries – Germany, Russia, Slovakia and Italy.[51] Machine tools were procured from European and Japanese suppliers.[52] Those working in the factory were allegedly unaware of the planned nuclear end-use for the products, as Urs Tinner took special efforts to safeguard all relevant documentation.[53]

The Khan case provides a starting point to consider the reasons for the exploitation of Malaysia by proliferators. Collins and Frantz note: 'Khan was intrigued because Malaysia offered a good technical base, lax export controls, and a location far from the spies and customs authorities of Europe and the United States'.[54] In 2004, Malaysia did not have a comprehensive export control system in place, and SCOPE's activities did not break Malaysian law. Malaysia was also a location less likely to cause concern amongst those supplying technology for the SCOPE venture.

[51] 'Transactions of Scomi Precision Engineering and Bikar Metal Asia, 2001-2002', undated, available at: (http://isis-online.org/uploads/isis-reports/documents/Transactions_of_Scomi_Precision_Engineering_and_Bikar_Metal_Asia_2001_to_2002.pdf) accessed 28 November 2017.
[52] Albright, *Peddling Peril*, p.135.
[53] Royal Malaysia Police, 'Press Release by Inspector-General of Police'.
[54] Frantz and Collins, *The Nuclear Jihadist*, p.261-2.

Hastings supplements the notion of limited regulation and a sufficient technical base with 'a social network to ensure the operation's success'.[55] He states: 'The choice of Malaysia … illustrates how Khan's network was constrained by the need for social ties and the political and economic characteristics of the countries in which it operated'.[56] He notes the centrality of Tahir in decision making, his residency status, shares in Scomi and political connections.[57] After the *BBC China* interdiction, Tahir left Dubai for Kuala Lumpur, allegedly expecting that 'his political connections would protect him', while Tinner packed up and fled Malaysia seeking to ensure little evidence was left behind.[58] These factors suggest the importance of personal connections and circumstances in third country selection.

In 2004, as a product of the Khan Network and broader concerns regarding WMD terrorism, the Security Council passed UNSCR 1540, requiring states put in place a series of measures to prevent WMD proliferation – including export controls, border controls and other measures. In its first 1540 report, the Malaysian government noted it lacked a

[55] Hastings, 'The Geography of Proliferation Networks', pp.429-50.
[56] Ibid.
[57] Ibid., p.443.
[58] Collins and Frantz, *Fallout*, p.87-89; Frantz and Collins, *The Nuclear Jihadist*, p.335.

comprehensive export control law.[59] New comprehensive legislation would not be put in place until 2010.

The SCOPE case suggests the choice of Malaysia was shaped by needing a location with lax regulation, a lack of oversight, and a supply of skilled labor. This saw Malaysia considered over Dubai and Turkey (insufficient workforce) and South Africa (perceived oversight). However, other countries could potentially have fulfilled these criteria. Existing personal connections of BSA Tahir and his belief that the country could provide political 'cover' played an important role in the selection of the country.

4. Iranian Procurement Activity in Malaysia

In the late 2000s Malaysia was an important transshipment hub for Iranian illicit procurement activity, with Iranian agents operating in the country to procure military and missile related goods. Leaked US State Department cables, US court documents and other

[59] 'Note verbale dated 26 October 2004 from the Permanent Mission of Malaysia to the United Nations addressed to the Chairman of the Committee', S/AC.44/2004/(02)/35, 4 November 2004, available at: (https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/594/24/PDF/N0459424.pdf?OpenElement) accessed 28 November 2017.

sources allow us to piece together a picture – albeit a fragmented one – of these activities. Malaysia has featured prominently in studies of Iranian illicit procurement. A US Government Accountability Office study noted that Malaysia or Singapore was involved in 20% of cases of Iranian illicit procurement of US origin military and dual-use goods.[60] This was only surpassed by the UAE which was involved in around 50% of the cases.[61] Another study presents slightly less evidence of Iranian use of Malaysia in nuclear-related illicit procurement.[62] However, Iranian activity in Malaysia in the late 2000s saw transshipment of electronics of use in Improvised Explosive Devices (IEDs), and aerospace and missile technologies.[63]

[60] Government Accountability Office, 'Iran Sanctions: Complete and Timely Licensing Data Needed to Strengthen Enforcement of Export Restrictions', Report Number GAO-10-375, March 2010, p.16.
[61] Ibid., p.17.
[62] 3 cases in Malaysia and 2 in 'Malaysia and Singapore' of 122 considered – Malaysia was much less prominent than China (38), UAE (13), and fewer cases than the US (6), Austria (5) and Spain (4). See Ian Stewart & Nick Gillard, 'Iran's Illicit Procurement Activities: Past, Present and Future', Project Alpha Report, 24 July 2015, available at: (http://projectalpha.eu/wp-content/uploads/sites/21/2015/07/20150724_-_Iran_Illicit_trade_past_present_future_FINAL.pdf) accessed 28 November 2017.
[63] With at least two exceptions – an unnamed Malaysian firm was implicated in efforts to procure Nuclear Suppliers Group controlled Russian-origin neutron generators. US Secretary of State, 'NIAG 8064: Iran Seeks Russian-Origin Neutron Generators through Malaysia', Cable No. 08STATE52481_a, 16 May 2008, available at; (https://wikileaks.org/plusd/cables/08STATE52481_a.html) accessed 17 May 2018. Nicholas Kaiga also plead guilty in a US court in 2014 of transshipping aluminum tubes (potentially of use in the manufacture of centrifuges) to Iran through Malaysia. US Immigration and Customs enforcement, 'ICE deports Belgian man convicted in Chicago of attempting to illegally export controlled nuclear non-proliferation items ultimately destined for Iran', 8 July 2015, available at: (https://www.ice.gov/news/releases/ice-deports-belgian-man-convicted-chicago-attempting-illegally-export-controlled) accessed 28 November 2017.

Following the coalition invasion of Iraq in 2003, Improvised Explosive Devices (IEDs) constructed using Iranian supplied components, were used extensively and claimed many casualties in the resulting insurgency. From at least 2006 until 2008, entities based in Malaysia were involved in a global procurement network sourcing key electronic components used in IEDs.[64] Malaysia-based, Iranian-operated, Vast Solution Sdn Bhd was involved in at least 12 procurements from US companies. These procurement efforts were linked to those of Dubai-based Mayrow General Trading Company, which had been operating since at least 2004. Procurement through the 'Malaysia conspiracy' increased after the efforts of Mayrow in Dubai seemed to tail off around 2006, with the Malaysian network gradually replacing the role of the Dubai network.[65] Vast Solution utilized direct Iran Air flights to transfer the goods to Tehran.[66]

In the same period, a wider network of Iranian front companies and procurement agents operated in Malaysia. In 2006, the UN Security Council put in place the first technology-

[64] United States District Court, Southern District of Florida, United States vs. Ali Akbar Yahya, F.N. Yaghmaei, Mayrow General Trading et al.
[65] David Albright, Paul Brannan, and Andrea Scheel, 'Iranian Entities' Illicit Military Procurement Networks', ISIS Report, 12 January 2009, available from: (http://isis-online.org/uploads/isis-reports/documents/IranMilitaryProcurement.pdf) accessed 28 November 2017.
[66] United States District Court, Southern District of Florida, United States vs. Ali Akbar Yahya, F.N. Yaghmaei, Mayrow General Trading et al., September 2008, pp.37, 40. All US court documents from Pacer, available at: (https://www.pacer.gov/) accessed 17 May 2018.

based sanctions on Iran's missile program.[67] At least ten entities and eight middlemen were operating on behalf of Iran in Malaysia during the 2008 to 2010 period.[68] These entities also operated in close connection to at least four in neighboring Singapore.[69] The US government noted this expanding Iranian activity in a 2008 paper on 'proliferation trends':

> Over the past several years, companies in Malaysia repeatedly have attempted to procure a variety of aerospace-qualified electronics from the U.S. and other MTCR Partner countries on behalf of military- and missile-related end-users in Iran. It also appears such companies …are expanding their procurement operations, regularly using multiple cover names and fraudulent end-user documentation, and routing their transactions through additional intermediaries to conceal the ultimate destination of an export.[70]

---

[67] UN Security Council 1737, S/RES/1737, 27 December 2006. This would be followed in 2010 by a full UN arms embargo. However, the overlap between goods of use in missile and aerospace programs, and broader US efforts to prevent Iran from obtaining US technology since the Iranian revolution, meant the US government expressed concern about Iranian illicit procurement much earlier.

[68] According to leaked US State Department cables – by no means a complete dataset, yet providing a snapshot. Only 7 of the 10 companies listed in the leaked cables were legally registered in the Malaysian company registry.

[69] Evidence from the cables – and United States District Court, Northern District of California, United States v. Majid Kakavand, April 2009, pp.9-10.

[70] MTCR refers to the Missile Technology Control Regime, a group of missile technology holding states which have harmonized export controls and exchange information on missile proliferation trends. US Secretary of State, 'Missile Technology Control Regime (MTCR): Missile Proliferation Trends', Cable No. 09STATE98749_a, 23 September 2009, available at: (https://wikileaks.org/plusd/cables/09STATE98749_a.html) accessed 17 May 2018.

These Iranian procurement networks operated in two interlinked clusters.[71] The first, was a cluster linked to the Iran-based Farazeh Equipment Distributor Company (FEDCO), an Iran-based supplier of SHIG (Iran's liquid fueled missile program) and the Iranian Unmanned Aerial Vehicle (UAV) program.[72] FEDCO has been described as a 'parent' company of Malaysia-based front companies Evertop Services Sdn Bhd and Elite Advanced Solutions Sdn Bhd.[73] FEDCO also employed Malaysia-based middlemen and brokers, including one which was seeking a data acquisition system of use in UAVs or satellites from a Belgian company.[74]

[71] Drawing on leaked cables, US court documents and other sources. There will likely have been other Iranian controlled entities and networks operating in Malaysia. The linkage between the two clusters is suggested in a cable which suggests that firms from both were both seeking the same UAV technology from a Japanese company – possibly working together or in competition. US Secretary of State, 'Iranian UAV Program Seeking Japanese-Origin Items via Malaysian Broker (S)', Cable No. 08STATE109147_a, 10 October 2008, available at: (https://wikileaks.org/plusd/cables/08STATE109147_a.html) accessed 17 May 2018.
[72] US Secretary of State, 'Iran's FEDCO Continues Efforts to Procure French Connectors from German Firm (S)', Cable No. 09STATE87162_a, 21 August 2009, available at: (https://wikileaks.org/plusd/cables/09STATE87162_a.html) accessed 17 May 2018.
[73] See for example US Secretary of State, '(S) Malaysian-Based Supplier to Iran Seeks Crystal Oscillators From Swiss Firm', Cable No. 08STATE101519_a, 23 September 2008, available at: (https://wikileaks.org/plusd/cables/08STATE101519_a.html) accessed 17 May 2018; US Secretary of State, 'New Information on Iranian Procurement Network's Efforts to Acquire German-Origin Items for Iran's Ballistic Missile Program (S)', Cable No. 09STATE19370_a, 3 March 2009, available at: (https://wikileaks.org/plusd/cables/09STATE19370_a.html) accessed 17 May 2018.
[74] US Secretary of State, 'Iranian Procurement Firm Continues Efforts to Purchase Belgian Data Acquisition Systems via Malaysia-Based Entities (S)', Cable No. 09STATE20617_a, 5 March 2009, available at: (https://wikileaks.org/plusd/cables/09STATE20617_a.html) accessed 17 May 2018.

Evertop's main customers were Iran Electronics Industry (IEI) which manufactures a diverse range of military goods including missile related goods and night vision equipment, and Iran Communication Industries (ICI) which manufactures military communications equipment.[75] Evertop was indicted by the US in 2009 for re-exporting 30 shipments of goods, largely consisting of electronic components, valued at over $1.18million.[76] Analysis of the products procured by Evertop, and the means used – including listing a freight forwarder as consignee—suggest that the scheme was an opportunistic effort to procure lower grade goods from naïve suppliers, rather than a sophisticated effort to target companies with significant Internal Compliance Programs.[77]

The activities of Evertop provide some insights into the choice of Malaysia. According to the Iranian nationals running Evertop, the company was a 'just a small private company stablished[sic] in Malaysia for the sake of shipment purposes only'.[78] When attempting to procure goods from US companies, they advised them that the end user was in Malaysia.[79]

[75] United States District Court, Northern District of California, United States v. Majid Kakavand, April 2009, p.11.
[76] Ibid., p.7.
[77] Clif Burns, 'Malaysia Fast Becoming a Diversion Destination for Exports to Iran', *ExportLawBlog*, 15 September 2009, available at: (http://www.exportlawblog.com/archives/566) accessed 28 November 2017.
[78] United States District Court, Northern District of California, United States v. Majid Kakavand, April 2009, p.9
[79] United States District Court, Northern District of California, United States of America V. Evertop Services SND BHD, Amir Ghasemi, Majid Kakavand and Alex Ramzi. 2009, p.6.

Apparently –as in the IED case– use of direct Iran Air flights was appealing, being consistently requested from freight forwarders.[80] Evertop also benefitted from the lax regulation of a Malaysian Free Trade Zone (FTZ).[81] FTZs have frequently featured in proliferation networks presenting a number of vulnerabilities.[82]

In 2008 Kakavand, an Evertop director, sought to establish new intermediate companies. Kakavand listed four generic company names in order of preference for an 'associate' to check in the registry.[83] The nonchalant 'please prepare the forms until we can sign them' suggests they faced little difficulty.[84] Indeed, registry data suggests Evertop was established with no problem by Kakavand and other Iranian procurement agents in 2005.[85]

The second cluster featured a series of companies surrounding Skylife Worldwide Sdn Bhd. A 2009 cable alleges that Skylife and, another front company, Microset Systems Sdn Bhd allegedly were 'co-located, work closely with one another, and have acted as brokers for

[80] Ibid., pp.8, 11.
[81] Ibid, p.15.
[82] Viski and Michel, 'Free Zones and Strategic Trade Controls'.
[83] These names were Vertex Technology Sdn Bhd; Zenith Technology Sdn Bhd; Summit Technology Sdn Bhd; Microsun Technology Sdn Bhd.
[84] United States District Court, Northern District of California, United States v. Majid Kakavand, April 2009, p.23.
[85] Data from the Malaysian corporate registry.

numerous Iranian entities of proliferation concern'.[86] One of Skylife's directors Mohammed Mahdavi was described by the US government as 'an Iranian procurement agent' and as having worked for SHIG, and Ya Mahdi Industries (an Iranian anti-tank and surface-to-air missile manufacturer).[87] Microset allegedly worked for a middleman linked to Fan Pardazan and Qods, both entities linked to Iran's UAV programme.[88] Both Skylife and Microset also supplied Iranian military aircraft manufacturer HESA.[89]

Enforcement cases provide insights into the operations of this aspect of the network. David Levick –an Australian businessman– allegedly procured goods from US companies and shipped them through a Malaysian company to Iran in 2007 and 2008.[90] While Skylife is not named in the indictment, reporting suggests that Levick's first contact with Iranian

[86] US Secretary of State, 'Malaysia-Based Procurement Entity Continues to Seek German-Origin Rotary Swaging Machine (S)', Cable No.09STATE115166_a, 6 November 2009, available at: (https://wikileaks.org/plusd/cables/09STATE115166_a.html) accessed 17 May 2018. The cables suggest these entities share an address. Searches of the Malaysian corporate registry did not reflect this.
[87] US Secretary of State, 'Malaysian-Based Front Company for Iranian Procurement Agent Seeks U.S.-Origin Equipment from South Korean Firm (S)', Cable No.09STATE104467_a, 7 October 2009, available at: (https://wikileaks.org/plusd/cables/09STATE104467_a.html) accessed 17 May 2018.
[88] US Secretary of State, 'Iranian UAV Program Seeking Japanese-Origin Items via Malaysian Broker (S)', Cable No.08STATE109147_a, 10 October 2008, available at: (https://wikileaks.org/plusd/cables/08STATE109147_a.html) accessed 17 May 2018.
[89] United States District Court, District of Columbia, United States of America v. Mac Aviation Group et al, 2009.
[90] Levick was indicted in 2011, but not extradited to the US. He was declared a fugitive in 2012, likely because of extradition difficulties.

middlemen was through the company.[91] The goods included gyroscopes, servo actuators, pressure transducers, an emergency floatation system, and a light assembly for various UAV, aircraft and helicopter applications.[92] In this case, Iranian middlemen transferred the goods so that they did not enter Malaysian customs territory, with a freight forwarder checking them and re-exporting them in Kuala Lumpur.[93]

In 2008 a complaint was issued against Skylife Director, Hossein Ali Khoshnevisrad, and his Tehran-based company Ariasa AG.[94] The complaint included charges that Khoshnevisrad had facilitated three shipments of 17 Rolls Royce helicopter engines from an Irish Company Mac Aviation to Iran via a Malaysian company.[95] In this case Khoshnevisrad used a separate front company, 'Pennerbit Kemas Sdn Bhd', a book trading company according to investigators.[96] This company appears not to have been registered,

[91] Paul Maley, 'Sanctions? What sanctions? Aussie accused of exporting goods to Iran', *The Australian* (2 March 2012)
[92] A list is provided in the indictment: United States District Court, District of Columbia, United States of America v. David Levick and ICM Components, Inc., 2011, p.7.
[93] Ibid., p.13.
[94] 'Affidavit in Support of a Criminal Complaint and Arrest Warrant, Hossein Ali Khoshnevisrad', August 2008. Confirmed in the Malaysian corporate registry.
[95] Ibid, p.3; United States District Court, District of Columbia, United States of America v. Mac Aviation Group et al., 2009.
[96] 'Affidavit in Support of a Criminal Complaint and Arrest Warrant, Hossein Ali Khoshnevisrad', August 2008, p.7.

and was likely just a false letterhead.[97] Mac Aviation also transferred other goods to Iran through Malaysia. Aircraft vanes – of use in jet engines – were shipped to Kuala Lumpur airport where they were also transferred onto a direct Iran Air flight to Tehran.[98]

By 2009, US officials suggested 'Malaysia was becoming the "new Dubai" for illicit traders'.[99] Despite US pressure, the new export control legislation had been 'floating about in the government, without any domestic champion or political will to push it to fruition'.[100] In April 2009 Najib Razak replaced Badawi as Prime Minister, and 'an unlikely but influential champion for strategic trade controls'.[101] The Strategic Trade Act (STA), passed in 2010, includes strong penalties for violators such as fines up to $7million or a death sentence for violations leading to loss of life.[102]

[97] Data from the Malaysian corporate registry.
[98] The indictment lists the flight number as IR841 – United States District Court, District of Columbia, United States of America v. Mac Aviation Group et al., 2009, p.22.
[99] US Embassy Kuala Lumpur, 'Malaysia: Special Advisor on Nonproliferation and Arms Control Robert Einhorn's Meeting with Senior Officials at MITI, Central Bank, and Atomic Energy Licensing Board, November 3-4, 2009', Cable No.09KUALALUMPUR917_a, 13 November 2009, available at: (https://wikileaks.org/plusd/cables/09KUALALUMPUR917_a.html) accessed 17 May 2018.
[100] M. S. A. Kareem, 'Implementation and Enforcement of Strategic Trade Controls in Malaysia', *Strategic Trade Review*, 2:2 (2016), pp.104-17.
[101] Ibid.
[102] Ibid.

In sum, Iranian procurement activities in Malaysia –for IED, UAV and missile technology– were extensive. Operations in Malaysia were underway at least a year before UN technology-based sanctions were put in place. However, Iran had been an embargoed destination for US technology since after the Iranian revolution, and subject to various other unilateral restrictions from other developed economies. There is little direct evidence to suggest why Iran chose Malaysia. However, investigation of these cases provides suggestions beyond a basic need to obscure the end user. The lax regulatory environment seems to be appealing, especially around heightened concern and the tightening up of controls in the UAE –Iran's most significant sanctions-busting hub– in 2007.[103] Iranian agents could establish new companies to conduct business with relative ease. Again though, besides the lax regulatory environment, present in most of East Asia, other factors may have contributed to the choice of Malaysia specifically. Malaysia, for example, provided the only direct Air Iran link to Tehran in South East Asia, which all the Iranian cases above utilized.[104]

[103] Karim Sadjadpour, 'The Battle of Dubai: the United Arab Emirates and the U.S.-Iran Cold War', Carnegie Paper, July 2011, p.21, available at: (http://carnegieendowment.org/files/dubai_iran.pdf) accessed 28 November 2017.
[104] Mahan Air also flew to Bangkok. 'Air Iran Route Map', October 2002, available at: (https://web.archive.org/web/20110515085921/http://airchive.com:80/html/timetable-and-route-maps/eurasia-middle-east/iran-air-october-27-2002/6659) accessed 28 November 2017.

5. North Korean Illicit Activity in Malaysia

Evidence suggests that Malaysia has long been a venue for North Korean arms trading, although two cases unearthed in early 2017, likely involving breaches of the UN arms embargo in place since 2006, provide more extensive evidence.[105] The activities of Glocom, said to be a 'Malaysia-based company' advertising 'radio communications equipment for military and paramilitary organizations', were featured in a 2017 UN report.[106] Glocom is described as a 'front company of the Democratic People's Republic of Korea company Pan Systems Pyongyang Branch'.[107] Two Malaysian registered companies

[105] A 2013 UN report suggested that British arms dealer Michael Ranger had held business meetings in Malaysia with North Korean dealers an unstated number of times since 2004. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2013/337, 11 June 2013. US officials travelled to Kuala Lumpur to warn banks that North Korean arms companies had Malaysian accounts in 2009. US Embassy Kuala Lumpur, 'Goldberg Delegation's Meetings with Malaysian Central Bank and Financial Institutions Re Implementation of UNSCR 1874', Cable No.09KUALALUMPUR549_a, 8 July 2009, available at: (https://wikileaks.org/plusd/cables/09KUALALUMPUR549_a.html) accessed 17 May 2018; A 2016 UN report also listed Malaysia as one country of a handful that KOMID (Korea Mining and Development Trading corporation, North Korea's primary arms dealing company) officials had travelled to between 2012 and 2015. UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2016/157, 24 February 2016.

[106] UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017. James Pearson & Roszanna Latiff, 'North Korea spy agency runs arms operation out of Malaysia, U.N. says', *Reuters* (26 February 2017) available at: (http://www.reuters.com/article/us-northkorea-malaysia-arms-insight-idUSKBN1650YE) accessed 28 November 2017.

[107] UN Security Council, 'Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)', S/2017/150, 27 February 2017, p.34.

(established in 2005 and 2012) acted on its behalf. The manufacturing of Glocom's radio equipment appears to have taken place in North Korea, and the procurement of components from mainland China and Hong Kong, and export of the finished product conducted using intermediaries based in mainland China, Hong Kong and Taiwan.

Pan Systems Pyongyang used Malaysia as a 'base for its key representative abroad', listing its website at a '.com.my' URL.[108] Malaysia may also have played a role as a transshipment or transit hub, with a shipment of radio gear being seized on route to a phantom end user in Thailand in 2011.[109] A 2018 UN report suggested Glocom's representative in Malaysia disclosed to a Malaysian bank that he intended to set up a factory in the country, although this was likely to justify opening an account.[110] The network was active recently, with a new Glocom website advertising new products going live in January 2017.[111] A recent

[108] Ibid., p.35, 155. '.my' is the internet country code top level domain for Malaysia.
[109] 'Malaysia says intercepted North Korean arms shipment to Thailand in 2011', *Reuters* (20 March 2017), available at: (http://www.reuters.com/article/us-northkorea-malaysia-arms-idUSKBN16R11U) accessed 28 November 2017.
[110] UN Security Council, 'Report of the Panel of Experts Established pursuant to resolution 1874 (2009)', S/2018/171, 5 March 2018, p.64.
[111] James Pearson & Roszanna Latiff, 'North Korea spy agency runs arms operation out of Malaysia, U.N. says', *Reuters* (26 February 2017), available from: (http://www.reuters.com/article/us-northkorea-malaysia-arms-insight-idUSKBN1650YE) accessed 28 November 2017;

brochure alleged that the company took $10mil annually from transactions in over 50 markets.[112]

A second case involves Kay Marine –a Malaysian boat builder– sanctioned by the US State Department in 2016.[113] A 2011 Kay Marine marketing video featured a number of North Korean-designed military craft including torpedo boats, semi-submersible vessels and a Yono Class miniature submarine. Statements by the company management in 2006 and 2007 suggest collaboration with North Korea in the 2000s, and the relationship may have involved the 'manufacture of assault boats'.[114] While there is evidence that Kay Marine marketed North Korean arms, and suggestion of possible collaboration in manufacturing, there is no hard evidence to suggest the vessels were manufactured in or transferred through Malaysia.

---

[112] 'Glocom and DPRK Fronts', *Armscontrolwonk* podcast, 10 March 2017, available at: (http://hwcdn.libsyn.com/p/9/0/6/906c3bf2ff3638e1/28.mp3?c_id=14476329&destination_id=228079&expiration=1500073227&hwt=58d46fb71bc5104af347016a346f398c) accessed 17 May 2018.

[113] Daniel Salisbury, 'A Malaysian Shipyard with North Korean Connections', *Armscontrolwonk*, 18 May 2017, available at: (http://www.armscontrolwonk.com/archive/1203180/daniel-salisbury-a-malaysian-shipyard-with-north-korean-connections/) accessed 28 November 2017.

[114] 'Boatbuilder Kaymarine gets more foreign orders', *The Star Online* (5 November 2006), available at: (http://www.thestar.com.my/business/business-news/2006/11/05/boatbuilder-kaymarine-gets-more-foreign-orders/#0wqmxpO2gHYx3253.99) accessed 28 November 2017; 'Seven More Marine Dept Boats To Provide Services', *Bernama* (March 5 2007).

Marketing conventional weaponry and related military equipment through entities based in 'third countries' is a modus operandi of North Korean arms dealers, allowing them to avoid scrutiny and pass off North Korean military products as goods produced by other countries. The cases involved companies that were to some degree taken over or 'controlled', rather than being established, by North Korean agents. North Korea often exploits existing business relationships and historical trading connections. These North Korean cases may not have involved the breach of export controls, because no goods are known to have been transferred through the country, and show how a wider landscape of legislation must be put in place in order to implement UN sanctions.

6. Why Malaysia? 'Third Country' Selection and Proliferation Network Behavior

Despite great differences between the cases, they all have at least one common factor: individuals, or groups, *decided* to exploit Malaysia as a 'third country' for proliferation purposes. This is rather than Malaysia featuring by default – for example through its ports due to its position in global transportation networks. This section further explores themes addressed in the cases above –laxly regulated environments and their genesis, as well as

other factors such as levels of development, logistical networks and existing social and political connections. It argues that Malaysia shares the 'commercial', but not the 'geographical', characteristics which Early suggests make certain third countries more likely to become trade-based sanctions busting hubs.[115]

Weak Regulation and Enforcement

A rationale which is evident in all cases discussed is the relative ease of doing business – in terms of export controls, other regulations, and limited oversight. Until 2010 Malaysia did not have a comprehensive export control system in place. Like most countries around the world, it has seemingly never successfully prosecuted a company or individual for breach of export controls.[116] In the cases explored, the Malaysian government has also displayed a general reluctance to act against proliferators.[117]

[115] Early, *Busted Sanctions*, pp.65-71; 77-9.
[116] Project Alpha, 'Countries That Have Prosecuted WMD Export Control Violators', available at: (https://public.tableau.com/profile/project.alpha#!/vizhome/GlobalWMDExportControlProsecutions/Dashboard1) accessed 28 November 2017.
[117] Although evidence is far from complete, all three cases explored above showed signs of government reluctance or inability to act –from legislative overhaul taking 6 years following the Khan revelations; limited enforcement action taken against the Iranian networks; and lack of evidence of investigation and action after the US government sanctioned Kay Marine.

While great advances have been made in Malaysia since the SCOPE case, issues remain in Malaysia's legal framework. For example, the Financial Action Task Force noted in 2015 that, 'Malaysia's technical gaps in relation to TFS [targeted financial sanctions] against the financing of proliferation are significant', with delay transposing new designations a source of concern.[118] It is unclear whether current Malaysian laws are fully in line with UN North Korea sanctions, and therefore whether the country is equipped to deal with the recent arms marketing cases. Although the STA does cover brokering, it is unclear what legal basis was used by Malaysian authorities to act on the Glocom case.[119] The 2017 collapse of the Chinpo Shipping trial in Singapore shows the challenges of prosecuting violations when domestic legislation does not exactly reflect the specific language of UN resolutions.[120]

[118] Financial Action Task Force, 'Anti-money laundering and counter-terrorist financing measures Malaysia', Mutual Evaluation Report, September 2015, available at: (http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Malaysia-2015.pdf) accessed 17 May 2018.
[119] Rosana Latiff, 'Malaysia says North Korean firms linked to arms trade being deactivated', *Reuters* (27 February 2017), available from: (https://www.reuters.com/article/us-northkorea-malaysia-arms/malaysia-says-north-korean-firms-linked-to-arms-trade-being-deactivated-idUSKBN167067?il=0) accessed 22 March 2018.
[120] Andrea Berger, 'The Chinpo Shipping Case Implodes', *Armscontrolwonk*, 15 May 2017, available at: (http://www.armscontrolwonk.com/archive/1203164/guest-post-the-chinpo-shipping-case-implodes/) accessed 28 November 2017.

Proliferators have likely exercised 'jurisdictional arbitrage' in choosing Malaysia because of its favorable national laws and regulations.[121] The peril of lax regulation, and the logic of deterrence and displacement when controls are tightened, clearly has currency in the US government.[122] The comment that Malaysia could become the 'new Dubai' reflects this logic. Dubai put in place export controls in 2007, around the time the IED smuggling network shifted emphasis to Malaysia. As one analyst from the policy community has noted, Iranian illicit procurement shifted from Dubai to Malaysia as a result of 'greater scrutiny'.[123]

The ease of establishing or registering companies also constitutes a factor contributing to the attractiveness of the regulatory environment, although evidence in the cases discussed is ambiguous. The Iranian cases seem to have involved front companies being established solely for re-export purposes. However, Iranian networks also involved companies which were not formally registered – merely letterheads.[124] In the Khan and North Korean cases,

[121] Williams, 'Transnational Criminal Networks', p.71.
[122] For example, US representatives noted 'Front companies and intermediaries involved in missile-related procurement often operate in countries with weak export control oversight and enforcement'. US Secretary of State, 'Missile Technology Control Regime (MTCR): Missile Proliferation Trends', Cable No. 09STATE98749_a, 23 September 2009, available at: (https://wikileaks.org/plusd/cables/09STATE98749_a.html) accessed 17 May 2018.
[123] Albright, *Peddling Peril*, p.201.
[124] It should be noted this doesn't necessarily indicate difficulty in establishing companies.

companies that had already been established were utilized. In the SCOPE case the company already existed and was renamed. The nature of the relationship between North Korea and Kay Marine is unclear, as is whether the owners of Malaysian surrogate companies of Glocom were aware that North Korean entities were using these businesses. A 2017 World Bank survey suggests that Malaysia is ranked relatively poorly for ease of establishing a business, perhaps suggesting why the Khan and North Korean cases involved already existing companies.[125]

Explaining the Regulatory Environment: Between Economics, Politics and Bureaucracy

If a weak or favorable regulatory environment drives proliferators' choices, what drives countries to develop such environments? Malaysia's regulatory environment can be viewed as a result of economic, political and bureaucratic factors. Following a series of structural reforms in the 1970s, Malaysia experienced significant economic growth facilitated by a favorable regulatory environment.[126] FTZs –established from 1972 onwards, and utilized in

[125] The country was ranked 111th of 190, compared to 24th for general ease of doing business. See World Bank, 'Economy Rankings', 2017, available at: (http://www.doingbusiness.org/rankings), accessed 27 November 2017.
[126] Koen, V. et al. *Malaysia's economic success story and challenges*, (Paris, OECD Publishing: 2017)

some of the Iranian cases above– formed a part of this.[127] In the 1980s and 1990s Malaysian ports also saw significant growth, competing with other regional players such as Singapore to create the most favorable atmosphere for business.[128]

All cases explored benefitted from a Malaysia's desire for international business. Elements of the Malaysian government have also prioritized economic growth over any political reservations. Government led-efforts to grow Malaysia's economic relationship with Iran were seen as UN technology-based sanctions were passed in 2006.[129] In 2007 a Malaysian government Minister suggested Malaysia could help to normalize Iran's relationship with the international community.[130] The following year, the country sent a delegation, including firms showcasing potentially sensitive technologies, to an Iranian trade show led by official government trade body Malaysia External Trade and Development Corporation (MATRADE).[131]

---

[127] Rajah Rasiah, 'Free Trade Zones and Industrial Development in Malaysia', in K. S. Jomo (ed.), *Industrializing Malaysia: Policy, Performance, Prospects* (London: Routledge, 1993).
[128] Michael Richardson, 'Malaysia Aims to Become a Key Southeast Asian Shipping Hub: Singapore Faces a Rival Next Door', *New York Times* (1 February 2002).
[129] UN Security Council 1737, S/RES/1737, 27 December 2006.
[130] 'Minister: Malaysia to assist Iran in normalizing position in global community', *Bernama* (8 November 2007).
[131] For example 'heat exchangers, pressure vessels, switchgears, electrical and electronic goods'. 'Malaysian Companies Seek to Increase Exports to Iran', *Bernama* (17 October 2008).

Around the time that Kay Marine appears to have started a relationship with North Korea – in the mid-2000s – the company's Managing Director spoke positively about international business.[132] As recently as 2016 – after the UN's imposition of sectoral sanctions on coal and iron exports – elements of the Malaysian government still openly pursued a greater trade relationship with North Korea.[133] In December 2016 the CEO of MATRADE sought to boost ties, stating 'North Korea is now looking at using Malaysia as a gateway to South-East Asian markets as it finds the country business-friendly with pro-business policies'.[134]

Malaysia's emphasis of disarmament over nonproliferation, and discomfort with tools such as sanctions and export controls may have also limited enforcement. Malaysia, it was noted in 2008 US government correspondence, while respecting UNSC resolutions, 'opposes use of sanctions as a means of diplomacy'.[135] In a statement in April 2004 debates about UNSCR1540, the Malaysian government suggested that the most effective way of preventing WMD terrorism was through nuclear disarmament, and expressed concern about

[132] 'Boatbuilder Kaymarine gets more foreign orders', *The Star Online* (5 November 2006), available from: (http://www.thestar.com.my/business/business-news/2006/11/05/boatbuilder-kaymarine-gets-more-foreign-orders/#0wqmxpO2gHYx3253.99) accessed 28 November 2017;
[133] UN Security Council 2270, S/RES/2270, 2 March 2016.
[134] 'Malaysia eyes boosting trade with North Korea', The Star (2 December 2016).
[135] US Embassy Kuala Lumpur, 'Malaysia Scenesetter for A/S O'Brien: Financial Controls', Cable No. 08KUALALUMPUR213_a, 26 March 2008, available at: (https://wikileaks.org/plusd/cables/08KUALALUMPUR213_a.html) accessed 17 May 2018.

the use of Chapter VII of the UN Charter.[136]

While Malaysia has slowly implemented export control reform, and has shown some reluctance in reining in business ties with Iran and North Korea and acting against their proliferation networks, Malaysia's relationship with the US has been an important regulating factor. For example, the government Minister speaking of normalizing relations with Iran in 2007 caveated it with, 'I think Malaysia is highly aware of the limits that it can do. We will not do anything to jeopardize our relations with the US'.[137] However, it was the entry into office of Najib Razak in 2009 that marked the start of a stronger and deeper bilateral relationship with the US.[138] Razak, as discussed, passed the STA in his first months in office, just before attending the US-hosted 2010 Nuclear Security Summit.

Limited enforcement action could also be explained by the challenges faced by the government bureaucracy in implementing a new export control system. These factors

[136] Chapter VII allows the UN Security Council to place legally binding measures on all member states. Malaysia was speaking on behalf of the Non Aligned Movement. Rastam Mohd Isa, Statement to the UN Security Council, S/PV.4950 (Resumption 1), available at: (http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/1540%20SPV%204950%20R1.pdf) accessed 28 November 2017.
[137] 'Minister: Malaysia to assist Iran in normalizing position in global community', *Bernama* (8 November 2007).
[138] Joshua R. Johnson, 'Cooperation and Pragmatism: Malaysian Foreign Policy under Najib', Asia Pacific Bulletin, No. 63, 3 June 2010.

suggest that limited enforcement is a result of inability rather than unwillingness. The Malaysian system has been in place just a few years, for example, and as one former official has noted, has only a handful of staff working on implementation.[139]

In sum, the shape of the regulatory landscape and enforcement efforts are a product of efforts to balance economic development, politics and security. This balance is sometimes regarded as a zero-sum game – that new efforts to enhance nonproliferation through regulation will impede economic development. Like many developing countries, Malaysia has traditionally been wary that an overly regulated business environment could harm economic development.[140] US and others have sought to highlight the positive aspects of creating a more regulated business environment, reducing risk for investors. For example, in 2010 the US highlighted that Malaysia's 'legitimate business interests would also suffer if it were seen as a "proliferators' playground".'[141]

[139] Kareem, 'Implementation and Enforcement of Strategic Trade Controls in Malaysia'.
[140] For example, a visiting delegation in 2000 reported: 'Malaysia was largely dependent on its trade, and was afraid that a comprehensive [export] control system would run counter to its commercial interest, which were Malaysia's principle source of income'. US Embassy The Hague, 'Readout on MTCR Dutch Chair Visit to South East Asia', Cable No. 00THEHAGUE1863_a, 22 June 2000, available at: (https://wikileaks.org/plusd/cables/00THEHAGUE1863_a.html) accessed 17 May 2018.
[141] US Embassy Kuala Lumpur, AA/S Van Diepen's Meetings in Kuala Lumpur on Non-Pro and Export Control Issues', Cable No.10KUALALUMPUR68_a, 5 February 2010, available at: (https://wikileaks.org/plusd/cables/10KUALALUMPUR68_a.html) accessed 17 May 2018.

Explaining Network Behavior: Beyond the Regulatory Environment

Malaysia's regulatory environment has limited explanatory value alone in explaining the proliferation networks' choices. Extracts of emails between procurement agents included in US court documents seldom refer to lax regulation.[142] It is also unlikely that those involved in these networks take such a structured approach to considering relative merits of different jurisdictions.[143] However, most importantly, the lax regulatory environment does not explain the choice of Malaysia over other relatively unregulated economies in South East Asia and beyond. When Malaysia put in place the STA in 2010, only Singapore out of ASEAN's 10 members had put similar legislation in place.[144] In terms of export controls, by 2010 Malaysia was actually one of the more regulated jurisdictions in the region. Other factors must supplement an explanation centered on a lax export control regulatory environment. These broader factors include features which distinguish 'hubs' from

[142] The lack of concern/ awareness expressed by these entities regarding regulation may be a reason they were caught or had their activities uncovered; or its importance in the choice of Malaysia may be obvious to those involved, and therefore not explicitly stated.
[143] For a discussion of the limits of the rational actor model, see Salisbury, 'Why do Entities Get Involved in Proliferation?', pp.306-8.
[144] Stephanie Lieggi and Richard Sabatini, 'Malaysia's Export Control Law: A Step Forward, But How Big?', 10 May 2010, available at: (http://www.nti.org/analysis/articles/malaysias-export-control-law/) accessed 28 November 2017.

‘havens’ –levels of development as reflected in the workforce, infrastructure and logistical connections– as well as existing social and political connections of those involved.

Basing a hub in a developed and industrialized economy provides a skilled workforce and helps proliferators to import required technology. In the SCOPE case, Malaysia was viewed as having a sufficiently advanced workforce when Dubai and Turkey couldn’t deliver. Kay Marine clearly had something to offer North Korean arms dealers, possibly in technical or procurement terms during alleged collaboration on assault boats, or in terms of an untainted and industrializing economy which could feasibly manufacture and therefore market these vessels without raising suspicion.

Orders for high specification products from a country with limited high-technology industry could raise suspicions about end uses and concern of possible transshipment risk amongst export controllers in government and industry in advanced economies. This factor likely was a consideration in the Khan and Iranian cases, which involved imports. States with previous nuclear aspirations could also raise concerns. For example, South Africa was initially discounted as an option by Khan and associates, because exports to the country might raise the interest of intelligence agencies. In the North Korean cases, Malaysia would

allow for the goods to masquerade as Malaysian. A less developed country could have been used to market North Korean military vessels and communications equipment, but this could have raised concern about quality, or because the product line was inconsistent with potential buyers' perceptions of the capability of the country's industry.

Good logistical and transportation links are clearly important in proliferator's location choices. Malaysia is a transshipment hub for legitimate global trade, like many other 'third countries' exploited by proliferators – for example, Dubai and the UAE, Hong Kong, Singapore and China. Malaysia is a part of major liner maritime shipping networks and has a large hub airport. Evidence of the importance of transportation links is clearer in the Iranian case. The three Iranian networks discussed saw goods re-exported on direct Iran Air flights to Tehran, making interdiction impossible once the goods left Kuala Lumpur International Airport, then Iran Air's only South East Asian destination. Factors such as access to infrastructure and the costs and time to trade across borders have featured – alongside other factors relating to regulation, compliance and legal protections – in the

World Bank's 'Ease of Doing Business' index.[145] Malaysia has consistently performed relatively well globally, and in the region in this index.[146]

While evidence of personal and political connections is lacking in the Iranian cases, there are clear examples in the Khan network and the North Korean cases. BSA Tahir's connections – through marriage in 1998, increasing association with the Prime Minister's son, and growing business interests in the country made Malaysia an obvious choice. His connections likely opened doors, and to an extent he believed they would protect him. In the North Korean cases, links to the Malaysian establishment – and that establishment interests have affected enforcement – should not be discounted.[147] Although it is unclear whether money changed hands, there was clear potential for 'corrupt protection' of proliferation networks in these cases.[148]

---

[145] The index includes categories such as 'getting electricity' and 'trading across borders', alongside 'paying taxes' and 'enforcing contracts'. See World Bank, 'Economy Rankings', 2017, available at: (http://www.doingbusiness.org/rankings) accessed 27 November 2017.

[146] For example, in 2017 Malaysia was ranked 24th globally of 190 countries, and 4th regionally behind Singapore, Hong Kong and Taiwan. Ibid.

[147] According to the Reuters reporting above prominent member of the UMNO Malaysian ruling party was listed as the director of one of the companies in the Glocom case; Kay Marine had a number of contracts with Malaysian government bodies, including for a research vessel funded by the Prime Minister's Department's Economic Planning Unit. Pathama Subramaniam, 'PAC wants graft probe on university's 'ailing' research vessel project', MalayMailOnline (27 October 2014), available from: (http://www.themalaymailonline.com/malaysia/article/pac-wants-graft-probe-on-universitys-ailing-research-vessel-project) accessed 28 November 2017.

[148] Matthew Bunn, 'Corruption and Nuclear Proliferation' in Robert I. Rotberg (ed.), *Corruption, Global Security and World Order* (Washington DC, US: Brookings Institution Press, 2009) p.136.

In sum, while there are clear differences between Early's concept of trade-based sanctions busting and the use of third countries in proliferation networks, there are also similarities in the characteristics of countries emerging as hubs for these activities. Specifically, as in the UAE example used by Early, Malaysia is an 'open' economy, with infrastructure to facilitate international trade.[149] However, Malaysia's pre-existing trade links with Iran and North Korea are less extensive than UAE's links to Iran. The Malaysian case explored undermines the importance of geographical proximity, which Early argues was important in the emergence of the UAE as a sanctions-busting hub.[150] That proliferation networks see the transfer of a small number of high-value shipments, rather than large volumes of trade, mean that geographical proximity and related low transportation costs are not as important in the emergence of third country hubs in proliferation networks. This agrees with arguments made in passing by Early and Naylor.[151] While geography is not such an important factor in the selection of third country hubs in proliferation networks, trade-based

[149] Early, *Busted Sanctions*, pp.68-9; 106; 122.
[150] Ibid, pp.77; 106; 122.
[151] See for example: 'circuitous routing provided an alibi and made countermeasures more difficult' in Naylor, *Patriots and Profiteers*, p.238; 'the sensitive nature of such transactions increases the value of discretion and/or opacity provided by particular third-party venues above the logistical advantages they offer' in Early, *Busted Sanctions*, p.102.

sanctions busting hubs often also see significant proliferation-related trade as well as trade volumes – for example the UAE in the case of Iran and China in the case of North Korea.[152]

7. Conclusion: Network Behavior and Nonproliferation Policy

This paper has considered the use of 'third countries' in proliferation networks to facilitate the transfer of WMD and military technologies. It has proposed a loose typology of ways which third countries are used in these networks –manufacturing, transshipment and brokering– and illustrated those using detailed case studies. In doing so, it has sought to provide a more nuanced conceptual grounding for discussion of proliferation networks. The use of a Malaysian cases has not been to single out the country –in theory any country can be exploited in such a way, and many have been– but to generate further insights into the decision-making of those involved in proliferation networks.

The paper has argued that explanations involving weak regulation and limited enforcement

[152] See Early, *Busted Sanctions*, p 120-2; John Park and Jim Walsh, 'Stopping North Korea, Inc.: Sanctions Effectiveness and Unintended Consequences', MIT Security Studies Program Report, August 2016, available at: (https://www.brookings.edu/events/stopping-north-korea-inc/) accessed 27 November 2017.

action need to be supplemented with other factors –social, political, bureaucratic, logistical and personal– to fully understand why those in illicit networks make the choices they do. The paper has sought to situate this question, and subsequent findings to contribute to the academic literature on proliferation networks and sanctions busting. Notably, it has found that while a different phenomenon to Early's trade-based sanctions busting, proliferation networks seek out hubs which share many of the characteristics of trade-based sanctions busting hubs. However, beyond this, our conceptual understanding of how illicit networks operate at the transactional level, and their geography is still underdeveloped.[153] Moving beyond a basic understanding of how illicit actors behave can provide an empirical basis to inform counter-proliferation strategies.

The importance of other factors highlighted in this study suggests that conducting further research into the relationships between policy tools such as export controls and the illicit activities they are designed to counter would be useful. Considering the question as to whether export controls and targeted sanctions are having the effects intended by policymakers complements new research which has highlighted the unintended effects of sanctions.[154] There also may be insights to gain from further exploration of the literature on

[153] Radden Keefe, 'The Geography of Badness', pp.99; 107.
[154] See for example Park and Walsh, 'North Korea Inc.'.

how legitimate businesses make their location choices. While data is limited, this article suggests it is still possible to extract insights.

Findings relating to the role of weakly regulated environments, and the importance of other factors such as personal connections, both suggest pessimistic outlooks for policy. There will always be spaces with less regulation and oversight than others– despite some significant successes in the implementation of the UNSCR 1540 agenda. This fact, paired with 'jurisdictional arbitrage' suggests that proliferation networks will merely be displaced by efforts to improve export controls and other legal tools, rather than eradicated. In this sense, efforts to improve the implementation of supply-side controls could be viewed as akin to a never-ending quest. That said, improvements in national export control systems could clearly increase detection and prosecution of these networks, as well as contributing to the development of a norm against illicit WMD-related trade.

On the other hand, focusing on the specific context of these networks and what drives their decision-making suggests that efforts to counter illicit networks should be heavily tailored. Although risk-based approaches to outreach are clearly important in prioritization efforts,

these findings highlight the limitations of indexes in considering third country risks.[155] Policy should be heavily intelligence driven and focused on disrupting illicit activity where prospects for deterrence is limited. More research should be conducted into unilateral means to disrupt these overseas networks for governments inclined to do so.[156] In the most prominent 'third countries' –namely China– progress on export control implementation and enforcement has been slow, and hostage to bilateral diplomatic relations. Both these types of approaches –enhancing legal frameworks and further developing the disruptive toolset – are undoubtedly required, and already being undertaken, by governments in their efforts to counter proliferation networks.

Acknowledgements

I am grateful for support and comments on earlier drafts received from colleagues at the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science and International Affairs: Matthew Bunn, Marty Malin, Will Tobey and Aaron Arnold. I am also grateful for the useful comments from the anonymous reviewers.

[155] For an example of this approach see David Albright et al. 'Peddling Peril Index (PPI) for 2017', ISIS Report, 31 January 2018, available from: (http://isis-online.org/isis-reports/detail/peddling-peril-index-ppi-for-2017) accessed 17 May 2018.
[156] See for example, Aaron Arnold and Daniel Salisbury, 'When Cooperative Counterproliferation Fails: Disrupting Overseas Illicit WMD Procurement Networks', forthcoming report, Spring 2018.

Biographical Information

Daniel Salisbury is a Research Fellow at the Centre for Science and Security Studies, Department of War Studies, King's College London. This article was researched and written during his time as a Stanton Nuclear Security Fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs.