Success and failure in nuclear proliferation network strategies

Justin V. Hastings

University of Sydney

Paper presented at the International Studies Association 2021 Annual Meeting (virtual), April 2021

Abstract

All proliferation networks use a menu of strategies, with varying success, to get around the attempts of non-proliferators to stop them. In this paper, I use a theory based on the economic geography of illicit transnational networks to explain North Korea and Iran's respective success and failure in building nuclear weapons. Both used similar strategies in their procurement networks: strategic structuring, obfuscation, and arbitrage of regulatory capacity. All these strategies trade off security and control for proliferators as they cooperate with non-state actors. While North Korea was able to use third-party brokers and arbitrage a number of different countries, Iran was forced into dependence on co-ethnic brokers and fewer transshipment countries. This resulted in territorially flexible North Korean networks that sacrificed some amount of security, and geographically limited Iranian networks that were relatively secure but susceptible to interdiction. The end result was North Korean success in proliferation network strategies, and Iranian failure. I conclude with theoretical implications for the study of illicit political economy and non-proliferation, and policy implications for non-proliferators.

Funding

The research for this paper was funded by the Australian Research Council (grants FT160100235 and DP140102098).

INTRODUCTION

As a result of its quest for weapons of mass destruction and the means to deliver them, North Korea has been subject to some of the most comprehensive sanctions ever imposed on a country. Between July 2006, when North Korea conducted several rounds of missile tests and the UN imposed sanctions for the first time, and November 2017, the UN Security Council passed 21 resolutions concerning North Korean proliferation activities, many of them imposing sanctions against North Korea or strengthening monitoring and enforcement of those sanctions.[1] By November 2017, North Korea had not only theoretically had its access to international financial institutions severely curtailed and its access to technology that could be used to build missiles, or nuclear, chemical, or biological weapons completely cut off, it had also been subject to export bans on seafood, textiles, and all manner of minerals, which had previously been the main legal source of income for the country.

North Korea's drive to continue its proliferation efforts, and its ability to maintain the networks that trade in restricted items, despite wave after wave of increasingly stringent sanctions, are a testament, if nothing else, to the sheer willpower of the North Korean leadership. But that North Korea could continue to persevere despite the sanctions, which were intended not only to express the international community's condemnation of the continued development of nuclear weapons and missiles, but also to actually retard that development, through the cut off of both financing and technology, speaks to the ingenuity and flexibility of its networks.

And in the end, despite all the sanctions, perhaps North Korea succeeded. In January 2018, when North Korea expressed a willingness to thaw relations with South Korea through participation in the Pyeongchang Winter Olympics, and again in April 2018, when the country announced its intention to shut down its nuclear test site near Punggrye-ri, it claimed that its move were done not out of desperation but because it had completed the development of its nuclear weapons and missile systems to its satisfaction, and did not need any more tests.[2] Why did North Korea succeed, despite decades of international community attention focused on making it fail?

The days of a state pursuing nuclear weapons using only its own resources are over – despite talk of a North Korean state proliferation network, North Koreans did business with a

[1] See UN site on DPRK-related resolutions.
[2] Anna Fifield, "North Korea says it will suspend nuclear and missile tests, shut down test site," *Washington Post*, 21 April 2018.

variety of private individuals and firms around the world, and the network that fed components and materials to and from North Korea could better be described as a hybrid cooperative network of state and non-state actors. As a result, we are interested in the process by which states collaborate with non-state actors, and the strategies they adopt, to acquire, transport, and sell, nuclear and dual-use technology. In this process, all proliferation network strategies come with trade-offs for the proliferator, not only in terms of the political and economic costs suffered by the proliferator, but also in terms of the structure and effectiveness of the networks. How states can manage these tradeoffs can lead to success or failure in running proliferation networks.

In this paper, I map out the networks of two cases of states attempting to proliferate – North Korea and Iran – and map out the hybrid trade networks used by each in a bid to understand the tradeoffs they faced and how they adapted to those tradeoffs. I find that Iran relied to a large extent on brokers that shared non-market ties with Iran, which increased security, but decreased flexibility, and rendered Iran susceptible to interdiction if the political and economic environment moved against it. By contrast, North Korea relied on third-country brokers, who were more flexible in both their own locations and their transshipment locations. While this decreased security, and increased North Korea's risk, this strategy allowed North Korea's network to be territorially flexible, thus allowing it to adapt to progressive attempts to shut it down.

A HYBRID STRATEGY FOR PROLIFERATION

An economic geographic approach to proliferation networks

A geographic approach to proliferation networks does not invalidate the traditional approach to proliferation so much as take it in a different direction, in two respects. First, a geographic approach attacks a different (and prior) element in the causal chains usually associated with network analysis in international relations. Second, a geographic approach uses conceptions of nodes and links based not only on the relationships of nodes to each other, but also on the relationships between nodes and links, and territory.

Traditional network analysis in international analysis is primarily concerned with how a network affects its external environment or, more relevant here, how the internal structure of the network – the relationships among the nodes -- affects the actors within the network and

leads to political outcomes.[3] With the geographic approach, I focus instead on how the nature of the network actors, and the spatial distribution of the technological and transportation infrastructure they use, shape the structure of the proliferation network, and more specifically, how it is physically arrayed across the world.

This analysis requires a rethinking of nodes and flows. Although there is nothing per se stopping links between nodes from being the physical movement of goods, in practice, most traditional network analysis in international relations takes nodes to be states or organizations (or, in the case of terrorist networks, individuals[4]), and the links between the nodes to be social or treaty relationships, or some other form of cooperation.[5] In his work on proliferation networks, for instance, Alex Montgomery treats entire countries as nodes, between which flow nuclear components and expertise.[6] This approach works well if it is governments themselves that are proliferating. In traditional proliferation rings, states are simultaneously the suppliers of technology and expertise, the coordinators (through government-to-government agreements) for the logistics networks that move goods between countries, and the buyers of that technology. There is little need to think about the logistics of cooperation because one state's decision to transfer technology directly to another state makes that transfer essentially a done deal (as opposed to tacit knowledge, as Montgomery points out).[7]

By contrast, the nodes of illicit transnational networks are people or organizations who are anchored in a specific piece of territory – a city, region, or country with a specific set of social, political, and economic characteristics. These characteristics shape and constrain the nodes and channel the movement of people, goods, and information.[8] Since the nodes and flows are both anchored in territory, of central importance to a geographic understanding of networks is not only where the nodes are, but how exactly the people, goods and information

---

[3] Emilie M. Hafner-Burton, Miles Kahler, and Alexander H. Montgomery, "Network Analysis in International Relations," *International Organization* 63 (Summer 2009).

[4] Valdis Krebs, "Uncloaking Terrorist Networks," *First Monday*, no. Vol. 7, No. 4 (April 2002); Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004); Justin Magouirk, Scott Atran, and Marc Sageman, "Connecting Terrorist Networks," *Studies in Conflict and Terrorism* 31 (2008).

[5] Hafner-Burton, Kahler, and Montgomery, "Network Analysis in International Relations."; Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders: Transnational Advocacy Networks in International Polictics* (Ithaca, NY: Cornell University Press, 1998).

[6] Alexander H. Montgomery, "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network," *International Security* 30, no. 2 (Fall 2005).

[7] "Stop Helping Me: When Nuclear Assistance Impedes Nuclear Programs," in *The Nuclear Renaissance and International Security*, ed. Adam N. Stulberg and Matthew Fuhrmann (Stanford, CA: Stanford University Press, 2013).

[8] Colin Flint, "Terrorism and Counterterrorism: Geographic Research Questions and Agendas," *The Professional Geographer* 55, no. 2 (May 2003); Susan L. Cutter, Douglas B. Richardson, and Thomas J. Wilbanks, eds., *The Geographical Dimensions of Terrorism* (New York: Routledge, 2003)., p. 151.

are being moved from point to point – over what kind of terrain, using what kind of transportation mechanism.[9]

Using an economic geographic approach, we can conceive of proliferation networks as global value chains,[10] with nodes physically located in both developed countries and emerging countries connected by multi-dimensional flows of information, money, and dual-use technology. These flows are coordinated and configured through the relationships between networks' nodes, which can consist of individuals, groups, actual firms, and state institutions.

Nuclear technology and materials are passed along chains of nodes at three levels – between individuals, between firms (of which individuals may be a part), and between countries. Analytically, it is most straightforward to treat a node as an individual embedded within a firm. Both the individual and the firm are, in turn, embedded in countries – the country in which they are physically located, and the country whose nationality they hold (which may not be the same as the country in which they might be located). This can lead to complex node characteristics: an individual of Iranian nationality located in the Netherlands might be working for a Russian firm located in the United States. Taking the network approach, and thinking of nodes as individuals embedded within firms moving technology, and materials between nodes, allows us to directly compare both fully state and fully non-state proliferation networks, as well as networks that fall somewhere along the considerable spectrum in between.

We can characterize proliferation networks along each of the four dimensions of the global value chain framework, asking a key question for each dimension. By answering these questions for each part of each network, we can characterize the network and understand its strengths and weaknesses.

What is being transferred within the network?

The *input-output structure* of the chain consists of the nodes (firms) within the chain that pass along information, services and resources while adding value between production

[9] This point has been made in the literature on areas of failed governance, and the opportunities they provide (or do not provide) for illicit groups to operate. See Angel Rabasa et al., "Ungoverned Territories: Understanding and Reducing Terrorism Risks," (Santa Monica, CA: RAND, 2007); James A. Piazza, "Incubators of Terror: Do Failed and Failing States Promote Transnational Terrorism?," *International Studies Quarterly* 52, no. 3 (2008); Justin V. Hastings, "Geographies of State Failure and Sophistication in Maritime Piracy Hijackings," *Political Geography* 28, no. 4 (May 2009); HARMONY, "Al-Qaida's (Mis)Adventures in the Horn of Africa," (West Point, NY: Combating Terrorism Center, United States Military Academy, 2007).

[10] Gary Gereffi, John Humphrey, and Timothy Sturgeon, "The Governance of Global Value Chains," *Review of International Political Economy* 12, no. 1 (2005); Gary Gereffi and Karina Fernandez-Stark, "Global Value Chain Analysis: A Primer," (Durham, NC: Center on Globalization, Governance & Competitiveness (CGGC), Duke University, 2011); Jeffrey Henderson et al., "Global Production Networks and the Analysis of Economic Development," *Review of International Political Economy* 9, no. 3 (August 2002).

(and the inputs) and the retail consumer. In the case of proliferation networks, the input-output structure is simply the groups, firms and individuals involved in producing, transporting, acquiring, and brokering dual-use technology, radioactive sources and nuclear materials. With both licit materials and dual-use trade, and illicit proliferation-relevant trade, we would expect the input-output structures themselves to look much like their counterparts in other sectors.

Where does activity take place within the network?

The *geographic scope* of the chain consists of the spatial distribution of those nodes at the local, national, regional, or even global levels.[11] Analysis of the geographical, political and social landscapes that undergird proliferation networks can reveal to what extent and in what way individual countries (or cities, or even facilities) are susceptible to illicit network penetration. The decisions made by buyers, suppliers and coordinators of nuclear materials and components are grounded in both their personal connections with the buyers and the location and structure of their supply chains. In this sense, the geographic scope of illicit networks is defined by their social connections, and the role of their host countries within global nuclear and dual-use trade networks.

How is the network coordinated and controlled?

The *governance structure* of global value chains consists of the 'authority and power relationships between firms that determine how financial, material, and human resources are allocated and flow within a chain'[12], or, in other words, how the chain is coordinated and controlled. Nuclear proliferation networks can be thought of as nodes of individuals, groups, or firms, located in specific countries, and connected by physical or social links.[13] Nodes involved in proliferation fall broadly into three categories: suppliers, coordinators (brokers), and buyers.[14] These three types of actors are connected by the physical movement of nuclear materials and components, as well as by their social connections (i.e. business relationships

[11] P. Dicken et al., "Chains and Networks, Territories and Scales: Towards a Relational Framework for Analyzing the Global Economy," *Global Networks* 1, no. 2 (2001)., p. 95

[12] Gary Gereffi and Miguel Korzeniewicz, *Commodity Chains and Global Capitalism* (Westport, CT: Praeger, 1994).pp. 96=97

[13] Our analytical goal is to map the physical movement around the world of components and material necessary for building nuclear facilities (sensitive, dual-use) and weapons, as well as the social connections between nodes that allow the logistical network to work properly.

[14] Lyudmila Zaitseva and Friedrich Steinhausler, "International Dimension of Illicit Trafficking in Nuclear and Other Radioactive Material," (Stanford, CA: Center for International Security and Cooperation, Stanford University, 2003); Lyudmila Zaitseva, "Organized Crime, Terrorism and Nuclear Trafficking," *Strategic Insights* 6, no. 5 (August 2007); Lyudmila Zaitseva and Kevin Hand, "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users," *American Behavioral Scientist* 46, no. 6 (February 2003).

and connections where they are subsidiaries of the same larger company). They are grounded "somewhere," (in some country) allowing us to map both physical and social networks onto territory.

Suppliers, in this case, include the companies that are the originators of the desired equipment, or the facilities from which material is supplied, and more generally, the countries in which these individuals and companies are located. *Buyers* include the actual end-users of the components or materials. These different types of actors then engage in economic transactions designed to move goods along the value chain and capture value, with relationships ranging from arms-length market relationships, which may persist over time, but where the costs of finding new partners is low, through intermediate types, to hierarchical relationships, in which the buyers and brokers have an in-house managerial relationship.[15]

Proliferation networks require coordinators, or *brokers*, who connect the suppliers and buyers, to operate correctly. We can think about two classes of coordinators. In the case of nuclear proliferation networks, *acquisitions brokers* consist of the individuals and firms that find suppliers and place orders for the components needed to build the facilities (i.e. centrifuges, reprocessing facilities, nuclear reactors) that produce useable plutonium or highly enriched uranium, and the materials needed to feed them. There may be two or more brokers within a technology acquisition chain, with one broker acting on behalf of the eventual buyer contacting the second broker that, in turn, places the orders. The acquisitions brokers act as agents of the buyers (particularly in the case of proliferation networks, where there are many potential sellers, but only a few potential buyers) or, less frequently, as agents of the sellers (when there is a seller determined to transfer equipment and material without having a specific buyer). Social brokers in nuclear proliferation networks connect acquisitions brokers through personal or business ties to both buyers and suppliers, but are not otherwise involved in technology or materials acquisition.

Technology and materials have to be shipped from the suppliers to buyers. The *transport brokers* facilitate the movement of components and materials on their way from origin to destination, and may serve as transshipment points for goods, taking delivery from sellers, and forwarding the goods on to the end-users. The transit points are the physical locations through which the components and materials pass on their way from origin to destination. The goods move between individuals (often employed by firms) of various nationalities, who are physically located in these countries. In some cases, the transport and

[15] Gereffi, Humphrey, and Sturgeon, "The Governance of Global Value Chains.", pp. 83-84.

acquisitions coordinators may be one and the same person or a company. In other cases, the acquisitions coordinators may be the nodes that contract with the transport coordinators (thus establishing a business link of their own) for transportation of the goods.

What environments do the network actors face?

Different types of nuclear proliferators are likely to face different *institutional environments,* in no small part because of the character of the goods they are buying, selling, and transporting, with social sanction, state regulatory and enforcement attitudes ranging from hostile to solicitous. In the case of nuclear networks, while nuclear materials are almost inevitably under strict transportation and export controls -- necessitating routes and methods that bypass state authority or use illicit means -- many nuclear- and dual-use components are commercially available to most buyers, and indeed, states may have an interest in promoting the sale and transport of such goods for economic development purposes, although the goods may still be subject to strategic trade controls. The difficulties that suppliers, coordinators, and buyers have in acquiring, transporting, and selling components are thus dependent on the laws and regulations of the countries through which the technology passes and the manner in which they are enforced (or not).

Both the individuals and organizations that are involved in proliferation have to be located somewhere. When Iran and Libya were doing business with AQ Khan, for example, Khan shipped centrifuge components through Dubai, not only because of its physical proximity to Iran, but also because he already had personal connections there and the country had crafted regulations to become a haven for expatriates and the largest transshipment port in the Middle East.[16] The decisions made by buyers, suppliers and coordinators of nuclear components are grounded in both their personal connections and the location and structure of their supply chains. This includes technological decisions; they cannot be understood without reference to a network's environment. Khan chose Malaysia to make the centrifuge tubes because of its precision manufacturing capacity *and* because that is where he had close social connections. Analysis of the environment that undergirds the acquisitions and transport networks, thus, can reveal to what extent and in what way individual countries (or cities, or even facilities) are susceptible to proliferation network penetration.[17]

[16] Douglas Frantz and Catherine Collins, *The Nuclear Jihadist* (New York: Twelve, 2007); Gordon Corera, *Shopping for Bombs* (Oxford: Oxford University Press, 2006).
[17] Justin V. Hastings, "The Geography of Nuclear Proliferation Networks: The Case of Aq Khan," *Nonproliferation Review* 19, no. 3 (2012).

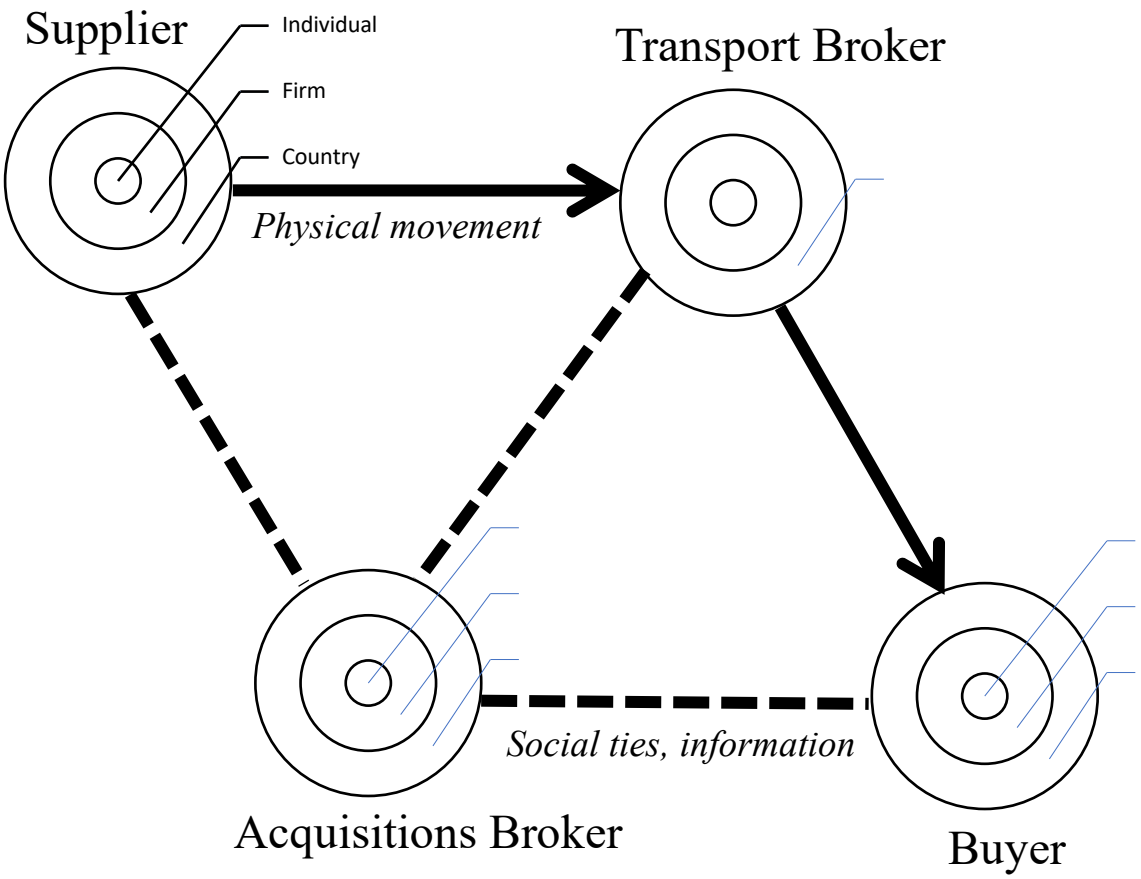

Figure 1. Conceptual diagram of a proliferation network

The fundamental challenge for proliferation networks

Growing attention to the "dark side" of social networks typically underscores the capacity of illicit sub-national groups to exploit new information technologies and globalization to create increasingly effective, flexible, and decentralized networks. [18] Technology, materials, and knowledge are generally assumed to flow freely among nodes. Yet the fundamental challenge for proliferation networks is that technology, materials, and knowledge *do not* flow freely between nodes. This is because transferring technology and materials in particular from one country to another in an environment where other countries, through the various mechanisms of the non-proliferation regime – supplier cartels, strategic trade controls, and general customs and anti-smuggling laws – are attempting to stop them. In

[18] Audrey Kurth Cronin, "Behind the Curve: Globalization and International Terrorism," *International Security* 27, no. 3 (2002-2003); Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (State College, PA: Pennsylvania State University Press, 2007); "Turning to the "Dark Side": Coordination, Exchange, and Learning in Criminal Networks," in *Networked Politics: Agency, Power, and Governance*, ed. Miles Kahler (Ithaca: Cornell University Press, 2009).

this environment, transferring proliferation-relevant goods is a problem that needs to be solved, and is not a foregone conclusion.

This is important because modern proliferation networks are liable to have non-state actors (a direct state-to-state transfer would not require entry into a market) or at least arms-length interaction between states. When a non-state actor such as a terrorist group or a private firm is involved, it is more difficult to assume that material and components will be transferred successfully, since these non-state actors may be at the mercy of potentially hostile states. While states directly engaged in proliferation can use their own transport resources, the non-state nodes in proliferation networks must rely on commercial infrastructure controlled by (often hostile) states to transit their materials across international borders.

What a geographical approach allows us to do, in essence, is to problematize the logistical challenges that proliferation networks might face. A proliferation network with logistical challenges to overcome is liable to look different, both structurally and how it is arrayed territorially, from one that has fewer logistical challenges. While the technologies of globalization – cheap, instantaneous communication, fast commercial shipping and transport around the world – theoretically free clandestine networks to move around the world outside the control of states, in fact the physical hubs for those technologies – container ports, transshipment hubs, airports, internet relay stations, and the like, are controlled by states, and are nexuses of state power and surveillance. This leads to a fundamental tradeoff – non-state actors engaged in illicit activities use the technologies of globalization at the cost of routing their movements through locations where states can interdict. Avoiding those hubs also increases costs and reduces the speed and efficiency at which the non-state actors can move.[19]

Confronted with this tradeoff, proliferators face four basic logistical problems: (1) where and how to buy proliferation-relevant technology and materials; (2) how to get goods out of the supplier country; (3) how to create routes to move goods around the world in the face of hostility from other states; (4) how to get the goods into the buyer country.[20] The structure of proliferation networks, and the strategies that proliferators use, are a result of how they attempt to resolve these problems.

---

[19] Justin V. Hastings, *No Man's Land: Globalization, Territory, and Clandestine Groups in Southeast Asia* (Ithaca and London: Cornell University Press, 2010).

[20] Alexander Kupatadze, "Organized Crime and the Trafficking of Radiological Materials: The Case of Georgia," *Nonproliferation Review* 17, no. 2 (July 2010); Andrew Prosser, "Nuclear Trafficking Routes: Dangerous Trends in Southern Asia," (Washington, DC: Center for Defense Information, 22 November 2004); Zaitseva and Steinhausler, "International Dimension of Illicit Trafficking in Nuclear and Other Radioactive Material."

Proliferation network strategies

Proliferators are likely to choose different proliferation strategies, each of which comes with their own sets of costs, benefits, and tradeoffs. The strategies are not mutually exclusive, and multiple strategies might be used across the network, or even by the same node within the network, depending on what problem the network is attempting to solve. Actors in proliferation networks may choose to use state resources and prerogatives, or they may choose obfuscation, strategic structuring of the network, arbitraging regulatory and production capacity and attention between states, or straight up smuggling.

In all strategies, there is a fundamental tradeoff between flexibility, security, and control for proliferation networks. Strategies that maintain security through a presumption of non-interference in diplomatic activities, and control through hierarchical relationships between the nodes in the relationship, and use of state transport infrastructure and diplomatic outposts, sacrifice flexibility in which nodes and links they can use, and where they can be located, and some security inasmuch as limited state-owned resources are relatively easy to surveil, but might gain some flexibility in how they move the goods. Strategies that accrue some measure of security and flexibility through hiding in plain sight in commercial routes and methods, and by using third-party brokers with market relationships and low transition costs, give up security and control inasmuch as proliferation networks' partners are substantially more likely to defect if they discover what is going on (or if they are discovered). At the same time, using the third-party non-state brokers with continuing links to the proliferation networks provides flexibility, inasmuch as the goods can move using commercial routes and methods that are not obviously connected with the proliferation networks, but the removal of those brokers can cripple the networks until they can find suitable alternatives.

While proliferation networks are not *per se* violent (at least not until they have acquired their nuclear bombs or radiological dispersion devices), in these tradeoffs, they bear some similarity to covert violent organizations such as terrorist groups or insurgencies, which also face a tradeoff between security, efficiency and control. The attempts of these organizations to address these tradeoffs (not always successfully) shapes the structure and behavior of the groups, and can explain what is sometimes seen as somewhat irrational behavior (such as well-funded terrorist organizations' operatives struggling with budget problems).[21]

[21] Jacob N. Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations* (Princeton, NJ: Princeton University Press, 2013); Jacob N. Shapiro and David A. Siegel, "Underfunding in Terrorist Organizations," *International Studies Quarterly* 51 (2007).

No proliferation network is obviously doomed to failure, nor is a network structured in a different way clearly destined for success. Nor does success or failure in the functioning of the proliferation network mean that all is well (or doomed) for the overall proliferation dreams of a state (or non-state actor): much more is needed to build a nuclear bomb, for instance, than simply acquiring the components to build uranium centrifuges and enough uranium to feed them. At the very least, states also need the technical knowledge, much of which is obtained through repeated social interactions, to run the machines and build the weapons.[22]

Given that proliferation networks face a series of challenges in operating, and the strategies they adopt to address those challenges all come with their tradeoffs in terms of benefits and risk, whether a proliferation network succeeds in moving technology and materials successfully from the supplier to the buyer is a matter of whether the network is able to avoid the risks inherent in their strategies, and pay the costs necessary to achieve success. In this, we can think of a number of 'fail points' – risks which may be especially difficult for proliferators to overcome if they actually eventuate, based on the strategies they use.

Given the downsides of what are obviously state actors and resources, proliferation networks have moved in the past several decades moved fairly decisively toward the use of non-state resources, or a hybrid of state and non-state resources, and have adopted a range of strategies. Much of the media perception of proliferation networks is that of "nuclear black markets," conveying an image of various shady characters trading missile parts and plutonium in a Middle Eastern bazaar.[23] In fact, when dealing with non-state actors in a proliferation network, the fundamental goal for proliferators is to keep as much of the network (apparently) licit as possible for as long as possible, and many proliferation strategies are by and large designed to accomplish this.

Suppliers, buyer, and brokers without access to state prerogatives and resources must set up support structures that depend on advantageous economic, political, and social characteristics of their host countries, and move their goods through economic and transportation infrastructure controlled by often hostile states. The result is that the territorial footprint of these networks hews to the legitimate 'commercial' landscape, moving through

[22] Philip Baxter, Adam Stulberg, and Justin V. Hastings, "Examining Subject Matter Networks of Tacit Knowledge Development: The Pakistan Nuclear Program Case Study," (Atlanta: Georgia Institute of Technology, 2016); Donald MacKenzie and Graham Spinardi, "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons," *American Journal of Sociology* 101, no. 1 (July 1995).

[23] David L. Albright and Corey Hinderstein, "Uncovering the Nuclear Black Market: Working toward Closing Gaps in the International Nonproliferation Regime," in *Institute for Nuclear Materials Management (INMM) 45th Annual Meeting* (Orlando, FL2 July 2004); Charles D. Lutes, "New Players on the Scene: A.Q. Khan and the Nuclear Black Market," *Foreign Policy Agenda* (March 2005).

commercial hubs and countries with favorable political, economic, and social characteristics, and must use strategies to obfuscate or otherwise throw off the investigations of states out to stop them. By hiding in the flow of commercial goods around the world, proliferators can make it more difficult for hostile states to detect their networks. At the same, the brokers are located in hostile states, and the goods are flowing through transshipment hubs or other central locations, which increase the vulnerability of the network if they are cut off. Moreover, because proliferators are putting their goods at the mercy of commercial infrastructure, and in some cases at the mercy of acquisitions and transport brokers with whom they do not have non-market ties, they sacrifice security and increase the risk of failure if they are detected.

While there are a range of strategies, or the purposes of this paper, I focus on the network configurations (as characterized by the diagrams below) created by differing obfuscation, arbitrage, and strategic structuring proliferation network strategies.

Obfuscation

Since state-owned resources, particularly those located in state-connected outposts (let alone in the state itself) are likely to be foci of attention by counter-proliferators, obfuscation of the true nature of the network is one strategy pursued by proliferation network actors.

First, the proliferation networks can obfuscate *the nature of the goods being traded*, and make them appear to be goods that are not in fact under sanction or are not subject to strategic trade controls. This could be accomplished simply by mis-declaring the nature of the goods on customs and shipping manifests, or by ordering breaking down items into components that are far enough removed from the main items that they are not readily identifiable as subject to controls.

Second, the proliferation networks can obfuscate the identities of the actors themselves. They might hide *their roles in the networks*, whether they are buyers, sellers, or transport or acquisitions brokers. This is crucial, since much of the technology and material trafficked in a proliferation network is not illicit, except when it is bought, sold, or brokered by a specific sanctioned individual, firm, or country. A broker that poses as a buyer or seller, essentially (if successful) moving the beginning of scrutiny one step away from sanctioned entities, is one way to do this. This strategy might be even more effective if the actor *separate the nationality* of the individual actor from that of the firm involved, and that of the firm from the country involved. In practice, this occurs when an individual works for (or more likely, directs) a firm located in a country different from his nationality, and when a firm incorporated in a country operates on behalf of another country. This strategy can also effectively disguise a state actor

as a non-state actor if, for example, the state actor creates a subsidiary in a different country that is controlled by individuals from the state actor parent.

An obfuscation strategy often means bringing in third-parties, or operating in third-countries, that may not have a close relationship with the proliferating actor. In this, the actor may trade off some amount of control for security, and may increase the risk that the partner will defect (since partners controlled by the proliferating state, or least partners who are co-nationals are less likely to defect) while decreasing the chance that the transaction will be discovered. In the extreme case, the proliferating actor may rely on market relationships, which increases the flexibility of the network (inasmuch as there are a large number of firms with which the network can partner) but also increase the risk of failure. On the other hand, relying on partners with whom proliferation networks have non-market relationships (either social ties, co-national ties, or state-controlled tied) decreases the risk of defection, but also decreases flexibility, inasmuch as the network is limited to actors with whom it has ties (who are often physically located in certain countries).

Arbitrage

In selecting and locating suppliers and transport and acquisitions brokers, the proliferation can arbitrage the difference in many countries between, on one hand, their lack of attention to non-proliferation, and imperfect (or non-existent) implementation of strategic trade controls, and on the other hand, their capacity to serve as supplier or broker countries. That they can take advantage of such a 'loophole' because rapid economic development and the spread of technical and industrial capacity in many domains relevant to proliferation have created a second (and even third) tier of countries that are not thought of as traditional suppliers of proliferation-relevant technology or materials. Moreover, the introduction of acquisitions, and particularly transport, brokers into proliferation networks means that even countries without any known capacity to supply proliferation-relevant technology or material can unknowingly participate in the operation of proliferation networks. The advantage for proliferation networks in arbitraging the difference between regulatory capacity and production/broker capacity is that fewer layers of subterfuge may be needed to accomplish their goals, and that layers of subterfuge that are used have a higher chance of working. In addition, countries used for arbitrage may not be the most obvious target for surveillance by hostile states, inasmuch as they are useful for arbitrage precisely because they are not among states traditionally thought of as being involved in global proliferation chains.

The risk of such a strategy is that the country being used as a supplier or a broker can become more hostile over time, as the country turns its attention to non-proliferation goals (either on its own, or at the goading of leading developed countries) and/or increases its capacity to regulate proliferation-related trade and production. The use of the country for proliferation purposes (whether brokering or supply) can of course itself cause the government to become more hostile or seek to build regulatory capacity. To the extent that the arbitraged country is host to individuals and firms with non-market relationships with proliferation network actors, the proliferation may sacrifice flexibility for some (temporary) amount of security and control over the supply and brokerage chain. As a result, a proliferation network that needs to operate over the long term must be flexible in its choice of arbitraged supplier or broker countries, and ready to move its operations to other countries. If it is unable to do that, this presents a problem for the network.

Strategic structuring

Proliferation networks can also strategically structure the routes and methods used to transport and acquire goods to make them more difficult to detect. Ironically, one way to do this is by, in combination with other strategies, following the standard global commercial shipping routes and using regular transport brokers (usually without knowledge of the nature of the goods, or the ultimate destination of the goods).

This has benefits for the proliferation network – transport costs are approximately what they would be for any 'regular' technology of material, and the lack of any particularly unusual movements (at least after the goods have left the supplier, and before they have arrived with the buyer) is less likely to raise alarm bells for counter-proliferators. The risk is that the goods themselves are easier to interdict, inasmuch as they follow normal global trade routes, and proceed through a relatively small number of transshipment hubs, and often through countries with relatively capable intelligence services. Routes that depend on transshipment hubs are also susceptible to being shut down if the hub is made unavailable. In addition, by relying to such an extent on market relationships with third party transport and acquisitions brokers, the proliferation network increases the chance that someone in the network will defect upon discovery.

Proliferators can also obfuscate the supplier and the ultimate destination of the goods by increasing the number of transport or acquisition brokers in the supply chain. This comes with risks as well, since every additional link in the chain not only increases costs and the time

in which the goods are out in the open, but also increases the number of hostile states who could interdict the goods or bring scrutiny to bear on the network.

Both the arbitrage and strategic structuring strategies are to a large extent dependent on the *availability* of geographically suitable countries, firms, and individuals. Obviously, a lack of willing buyers in viable countries can impede the ability of an inward proliferation network to acquire materials or technology. Likewise, the removal of strategic countries from the network – for example, a transshipment hub, or a country with regulatory arbitrage – can significantly impede the network's goals if there are not viable alternatives. This can be a particular problem for proliferation networks that are in hostile neighborhoods: if only one country in a region is viable transshipment hub, for example, the loss of that country may be particularly devastating. Similarly, if there are no countries physically near to a proliferating state that have the right combination of technological development and benign neglect of non-proliferation goals, the proliferation network is likely to face difficulties, and may have to move on to other strategies.

Successful and failure

While the framework is not intended to predict which proliferation networks will succeed or fail as a whole, it can help us to understand why, given certain constraints, proliferation networks are structured in the ways that they are, and lay out the costs and benefits of the different strategies they pursue to circumvent attempts by hostile states to stop them from buying, selling, or brokering proliferation-related technology and material. These strategies in turn tend to lead proliferation networks to have certain territorial layouts, and to exhibit certain strengths and weaknesses, some of which may be exploited by those involved in non-proliferation enforcement.

When proliferation networks succeed, or perhaps more accurately, when one or several chains within a larger campaign to buy, sell, or broker trade in proliferation goods or materials succeeds in moving the wares from the beginning to the end of the chain, it is because they have found ways to address the tradeoffs that come with different proliferation strategies, and those gambles have paid off (at least up to that point), and because their implementation of proliferation strategies have successfully minimized the costs inherent in those strategies. When the proliferation networks fail, it is because they are unable to overcome the weaknesses that are inherent in the strategies that they have chosen to facilitate proliferation. The tradeoffs they make end up costing too much relative to the benefits, or because the weaknesses end up being holes that the proliferator is unable to fill, and that hostile states can exploit.

Cases

Iran

Iran is a useful case study to look at success and failure in proliferation networks for several reasons. First, given how active Iran has been in attempting to subvert nuclear and other sanctions, and given the prolonged nature of the sanctions enacted against it, there is considerable information about the networks set up by Iran to bring components and expertise into the country (although like all clandestine programs, that information is still incredibly patchy). Second, because Iran has faced relatively comprehensive sanctions, particularly from the United States, with a reprieve during the JCPOA era, it has had to build clandestine networks to acquire almost *any* advanced technology (not to mention on occasions to sell oil).

By and large, Iran's inward proliferation networks can be characterized as hybrids: non-state suppliers connected to state buyers through state or non-state brokers, depending on the particular transaction. Iran's nuclear proliferation network is thus a classic example of a hybrid proliferation network, one which incorporates both state and non-state elements at different points in the chain from supplier through coordinator to buyer. While the early phase of Pakistan's quest for nuclear weapons was largely a state enterprise, with state buyers relying on state coordinators who used diplomatic prerogatives and state transportation resources to move goods from sellers to Pakistan,[24] Iran has been unable to pursue such a blatant path to the bomb. It is in how Iran has attempted to deploy these hybrid assets in pursuit of proliferation that it foundered for many years.

North Korea

North Korea offers an important comparison with Iran, inasmuch as it has also run a nuclear proliferation network for decades. Unlike Iran as of 2020, North Korea has successfully built and detonated multiple nuclear weapons, up to and including a hydrogen bomb. There is significantly less information about North Korea's attempts to acquire nuclear and dual-use materials and components than there is for Iran. As with Iran, because North Korea faces comprehensive sanctions, it has had to build clandestine networks to acquire almost *any* advanced technology, particularly as the scope of sanctions has spread into conventional technology and materials that could even theoretically be used for its weapons programs.

[24] Hastings, "The Geography of Nuclear Proliferation Networks: The Case of Aq Khan."; Steve Weissman and Herbert Krosney, *The Islamic Bomb: The Nuclear Threat to Israel and the Middle East* (New York: New York Times Books, 1981); Al J. Venter, *Allah's Bomb* (Guilford, CT: The Lyons Press, 2007).

I look at *how* North Korea's proliferation efforts have succeeded where Iran's floundered. Like Iran's, North Korea's proliferation network, at least since the end of the Cold War, has become hybridized, with state brokers interacting with private suppliers, or with state actors employing non-state brokers to conduct business on their behalf and transport the goods much of the way toward North Korea. However, in the operation of these hybrid proliferation networks, North Korea has demonstrated a willingness to accept high levels of risk, and move between different strategies and partners as needed. Paradoxically, we can see much of the ingenuity of North Korea's proliferation networks deriving from the evolution of North Korea's economy since the end of the Cold War, and particularly since the Arduous March, the great famine in North Korea in the mid-1990s: North Korea's proliferation strategies are in some sense extensions of how North Koreans do business in general, which makes them particularly difficult to stop.[25]

Network analysis

For this paper, I map out the networks Iran and North built up to import dual-use and otherwise banned items from (largely private) suppliers. In both cases, the information for the networks comes from media reports, academic accounts, United States and European reports of prosecutions for sanctions violations as well as United Nations reports on sanctions violations. The time frames for the networks for Iran are from the 1990s to 2018, while the time frame for North Korea is from the late 1980s to 2018. While North Korea imported a significant quantity of luxury goods (which were sanctioned by at least some countries), and the firms that were involved in importing luxury goods were also often involved in importing dual-use items, for the sake of simplicity and comparability with Iran, I excluded those networks from this particular paper.

For the network graphs, a node is defined as an individual embedded in a company embedded in a country. Both the individual and the company have both nationalities and locations. Given that these are often covert transactions, there is a significant amount of missing information, and we have to make judgment calls about coding the nodes. A company located in that country is assumed to have the nationality of that country unless otherwise stated. A company tied to an individual is assumed to have the nationality and location of the individual's location unless otherwise stated. Where an individual is not named for a company, the

[25] Justin V. Hastings, *A Most Enterprising Country: North Korea in the Global Economy* (Ithaca and London: Cornell University Press, 2016).

individual is assumed to have the same nationality and location as the company (if those are named for the company). Where an individual has dual nationality, the nationality that is *not* the same as the country in which he or she is located is coded. If there was another company heavily implied in the description of the transaction (for example, an item is listed as being supplied from an unnamed company in the US, or a good is listed as being transported through the UAE with no transshipment company named), I added an implied company labeled as, and coded to, the implied company location.

An edge is defined as a connection between two nodes with two major characteristics: the nature of the relationship, and what is being transported or transacted. There are four types of relationships represented by an edge: (1) *business*, in which the nodes are contracting to buy or supply items (and may transport them); (2) *transport*, which reflects the actual physical transport route of the goods, when there is no other relationship between the two nodes (that is, the buyer and supplier are linked by a business edge, but the goods are transported through an otherwise unrelated logistical company); (3) *subsidiary*, where there is an ownership relationship between two nodes ; (4) *social*, where the two individuals within the two nodes have a non-business relationship that is not captured by other types of relationships.

In the case of North Korea, this approach produced 142 nodes and 144 edges, with 42 transactions (and a somewhat smaller number of separate networks). In the case of Iran, I derived 562 nodes, and 695 edges, with 126 separate networks (some of which had multiple transactions). The inclusion of the transactions intended to import luxury goods into North Korea would add some networks. With that said, the disparity in data (over approximately the same time period) is likely more due to data availability, and the ability of the US and the UK to prosecute Iranian transactions relative to North Korean transactions (which may avoid the US entirely), than a significantly less active North Korean program to evade sanctions.

NORTH KOREA'S SUCCESS

A menu of strategies

As with Iran, North Korea made use of the full range of proliferation strategies. North Korean state prerogatives and resources have long been turned toward supporting the North Korean state's drive to bring in revenue through exporting proliferation-relevant technology, and to bring in components that can support their weapons programs. North Korean diplomats are tasked with raising their own incomes through business, as well as money for the

government, while North Korean diplomatic outposts and company branches around serve as the focal points for North Korean state actors' social and in some cases logistical networks.

With increasing UN sanctions and international scrutiny, the role that North Korean diplomats and their outposts have played in the proliferation networks has changed, from one in which the outposts themselves funneled goods and money, often physically, toward one in which diplomats serve as both transport and acquisitions brokers, often without ever touching the goods, and the outposts serve as the putative locations of front companies that serve as the formal loci of brokering, although North Korea has also taken advantage of individuals and companies in foreign locations that are organizationally and territorially divorced from diplomatic outposts.

North Korea, to a greater extent than Iran, selected countries as suppliers and brokers that provided a combination of indifference to North Korean activities (or inability to enforce sanctions and other relevant regulations), and technological, industrial, or transport capacity that would allow North Korea to route its proliferation networks through the country. North Korea was in the fortunate position (unlike Iran's conflict with many Sunni-ruled countries and Israel), where, outside of Northeast Asia and the US, few countries had an ideological or religious reason not to deal with North Koreans, particularly before sanctions began to ban many types of ostensibly legitimate trade.

As with other countries, North Korea also obfuscates the nature of the goods and technology it is trading through false customs declarations, and hides the identity of its individuals and companies as North Korean through a combination of front companies, false identities, and perhaps most importantly, using companies and individuals that are not in fact North Korean or often even located particularly close to North Korea. North Korea's obfuscation strategies are thus intimately tied to its strategic structuring of its networks. In recent years, this structuring has led North Korea to emphasize the use of commercial routes and methods for the transport of goods (at least to and from the first stop after or the last stop before North Korea), and to minimize the role of North Korean actors for as long as possible as proliferation goods pass down the chain.

Characterizing North Korea’s networks

The diagrams below show how North Korea’s obfuscation, arbitraging and strategic structuring strategies played out across its network over a thirty year period. Figure 2 shows North Korean import networks (clustered by transactions, either a single transaction or related

transactions), colored by the *location* of the firm embedded in the node. Because these are import networks, all networks should in theory end inside North Korea. *How* they get there is another matter. While North Korea is capable of sourcing and transshipping goods from outside of Taiwan, China, and Japan, as indicated by its nodes' connections with gray nodes, a majority of networks have Taiwanese, Chinese, or Japanese broker nodes, as either the acquisitions nodes for North Korean buyers, or the transshipment nodes on the way to North Korea, or both.

Figure 3, which shows the nationality of the firms (that is, whether the firm is actually from the country in which it is located, or whether it is registered or actually based somewhere else), suggests that there are some situations in which North Korean firms are operating out of other countries, or in which third-country firms are operating out of countries that are foreign to them (such as a Chinese firm operating in Hong Kong, or a Dutch firm operating in Singapore). To a certain extent, this would be expected in a globalized world. It does suggest, however, that there are a substantial number of third-country, multinational firms that are dealing with North Korean trade.

This is further confirmed in Figure 4, which shows the nationality of the individuals operating in different firms. The diagram shows that North Korean nationals are not particularly numerous outside of North Korea; instead, there is a general alignment of individuals' nationality and group location outside of North Korea. This suggests that, while there are indeed networks in which North Korean brokers are operating out of other countries (particularly Japan before 2009), by and large North Korean acquisitions networks are done by third-country nationals operating outside of North Korea.

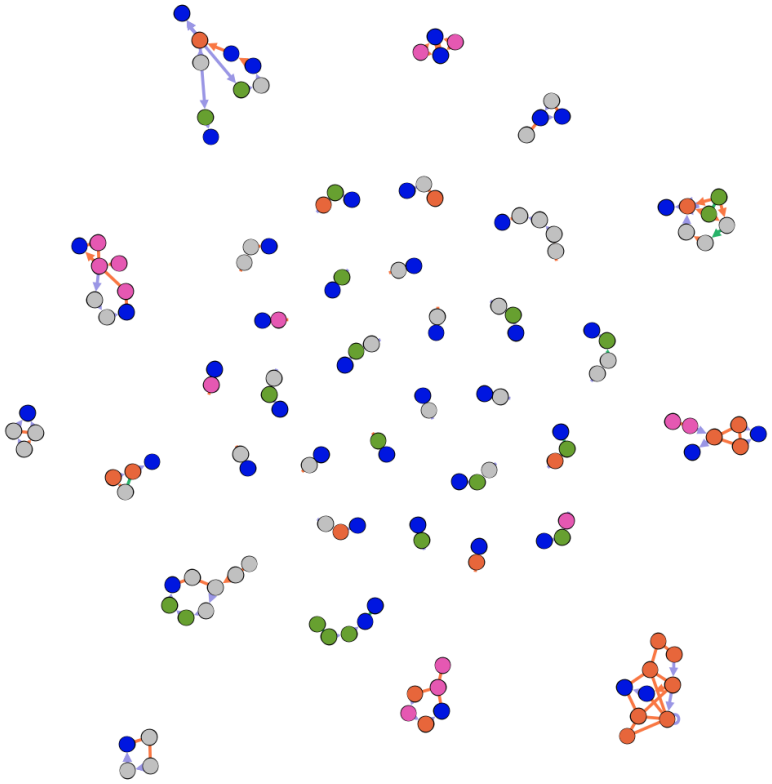

Figure 2. North Korean import networks, with group location highlighted (North Korea = blue; China = green; Taiwan = orange; Japan = pink; others = gray)

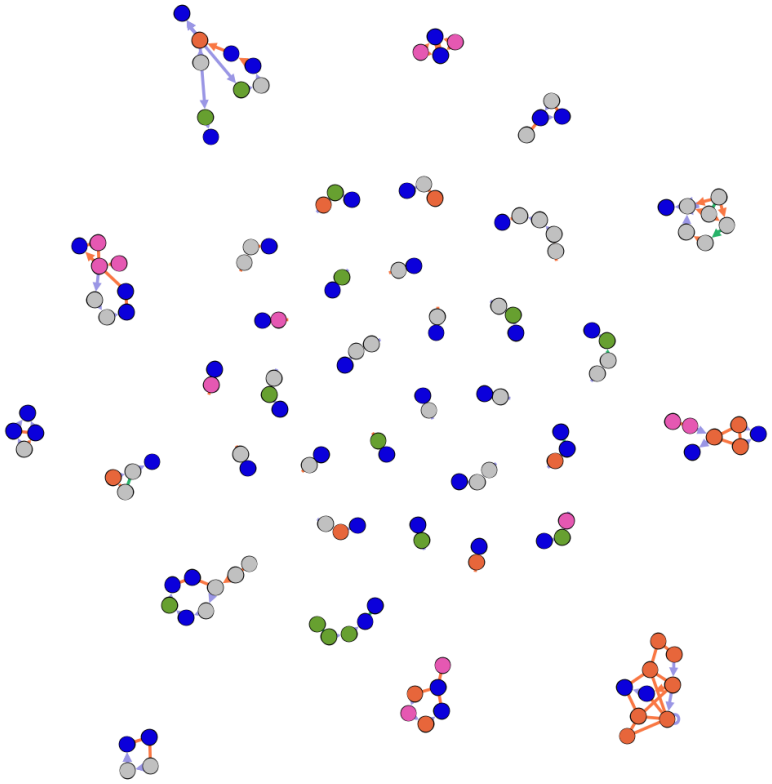

Figure 3. North Korean import networks, with group nationality highlighted

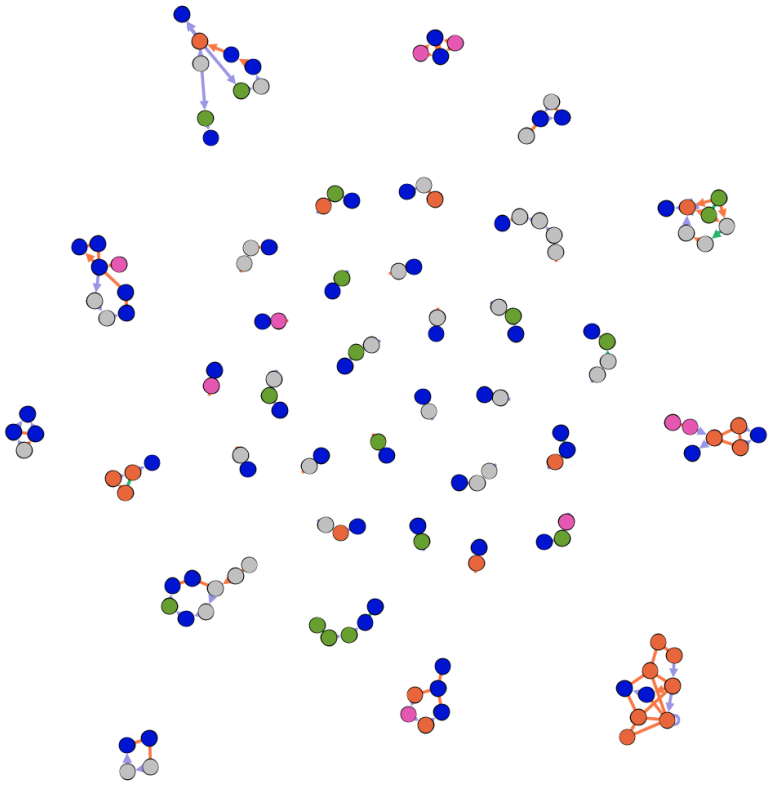

Figure 4. North Korean import networks, with individual nationality highlighted

There are two distinctives about North Korea's inward proliferation networks that can be drawn from North Korean import network diagrams. First, North Korea used at least three different brokerage countries over time – Japan, Taiwan, and China – suggesting that it had a certain amount of flexibility in how its goods got to North Korea, and that it was able to adapt its routes and methods as conditions changed. Japan, for instance, significantly cut down on trade with North Korea in 2006, and completely cut it off in 2009, which eliminated Japan as a useful brokerage country for North Korea. Taiwan is not part of the United Nations at all, and thus not legally subject to UN sanctions, although it generally aligns its laws, regulations, and enforcement actions with United Nations sanctions resolutions and the Non-Proliferation Treaty. As for China, the vast majority of North Korea's legal, formal trade comes through China; it is likely that most of its illicit trade does as well. Yet because the rigor with which China enforces United Nations sanctions varies over time and with the warmth of China-North Korea relations, North Korea must find other transshipment points as well, which is perhaps

why Taiwanese brokers continue to figure in North Korean import networks (particularly for ship-to-ship oil transfers).[26]

Second, aside from having multiple brokerage/transshipment countries, the alignment of individual nationality, group nationality, and group location suggests that North Korea's suppliers and brokers are largely non-North Korean businesspeople running businesses from their own (or other convenient countries). North Korea's proliferation network, in other words, is actually not particularly North Korean, nor, except for the initial outreach to acquisitions and transport brokers, are North Korean individuals necessarily involved in pursuing the different proliferation network strategies.

The key to North Korea's success

North Korea's ultimate success in deploying its proliferation strategies was based in large part in *how* it deployed those strategies. While North Korea is often thought of as being an isolated, paranoid state, in fact, it is surprisingly well integrated into the global economy in the practices and networks that are relevant to proliferation.[27] Inasmuch as integration is understood in a proliferation network as being a situation where a large proportion of the network is outside the proliferating state's territory and does not involve nationals or firms from the proliferating state, North Korea was arguably *more* integrated into the relevant parts of the global economy than Iran, despite Iran's higher levels of general economic integration (and susceptibility to economic sanctions).

This integration showed up in the proliferation networks' structure and behavior as a situation where North Korean actors often did not have to resolve the problems associated with using a given strategy because they were not actually involved in the network. North Korea essentially solved many of the problems of proliferation by getting other countries to do its work for it as far down the chain as possible, with identifiably North Korean actors only needing to solve the final-mile/first-mile problem. The prominence of third-country brokers in inward and outward proliferation networks, and the ability of North Korean actors to serve as brokers for networks that never physically touched North Korea reinforces this point.

Placing the operation of so much of the network into others' hands sacrificed control, and some aspects of security. North Korea addressed this tradeoff in a number of different

[26] Panel of Experts, "Final Report of the Panel of Experts Submitted Pursuant to Resolution 2345 (2017)," (New York: United Nations Security Council, 5 March 2018).
[27] Justin V. Hastings, *A Most Enterprising Country: North Korea in the Global Economy* (Ithaca and London: Cornell University Press, 2016). See Chapter 2.

ways. First, North Korea was willing and able to shift from high-trust non-market relationships between the nodes in its networks to market relationships as the situation warranted. Transactions that had previously taken place between North Korean firms or individuals were shifted to North Koreans interacting with third-country brokers and suppliers who maintained non-market ties with North Korean actors, or at least relationships that survived multiple transactions. Further down the chain, North Koreans showed themselves willing to engage in market-based transactions, despite the higher risk of failure and compromise.

North Korea also showed flexibility in its ability to arbitrage multiple countries as suppliers or transport or acquisition broker locations over time, in response to changes in the external political environment, particularly other countries' awareness of North Korean activities and willingness to crack down. North Korea used North ethnic Korean or third-country national brokers first in Japan, then Taiwan, and then finally China. Outside of Northeast Asia, North Korean brokers managed to operate through a number of countries in Southeast Asia, including Thailand, Malaysia, and Singapore, in the networks' dealings with foreign suppliers and brokers. As a result, the actual paths that the goods would take to and from North Korea, and the identities of the networks that would support those transactions, were not necessarily obvious, despite North Korea's use of commercial routes and methods for nearly the entire length of the chain.

North Korea also demonstrated flexibility in its ability to shift between state assets and non-state assets so as to obfuscate the nature of the networks. The use of non-state brokers, particularly third-country acquisitions brokers, is an example of this, as is the shift from using North Korean state transportation assets to hiding goods in commercial shipments. So too is the shift in the use of North Korean diplomatic outposts and diplomats as acquisition and transport brokers to seemingly private firms operated by North Koreans in foreign countries.

North Korea's implementation of the proliferation strategies, and the success thereof, were largely paralleled in the practices, actors, and patterns that had developed since the end of the Cold War in North Korea's domestic economy and external general trade networks. In many cases, the proliferation trade networks were no different from the general trade networks in their strategies, or even in terms of the individuals and firms involved. To say there were trade networks devoted to proliferation is perhaps misleading: the networks engaged in proliferation were a subset of the networks engaging in all manner of activities designed to support North Korea. The flexibility of North Korea's proliferation networks, the ambiguity of the status of many North Korean actors, and the acceptance of high levels of risk, were all

characteristics of North Korean trade networks more generally. North Korean actors were willing to trade off security and control in favor of flexibility in most aspects of the proliferation networks' operation and structure: in their partners, locations, and methods used to get around sanctions and hostile enforcement.

IRAN'S FAILURE

A menu of strategies

As with other proliferation networks, Iran's network made use of a number of strategies to attempt to (in most cases) acquire dual-use components for its nuclear program, and to a lesser extent, to supply missiles and weapons to other actors. First, Iran made use of state prerogatives and resources. Iranian government-owned ships and planes, in particular, transported missile and dual-use components between Iran and other countries. Iran government agencies and state-owned companies created subsidiaries and front companies. Unlike with North Korea, Iran does not seem to have made significant use of its embassies and diplomatic outposts directly as economic agents.

Second, Iranian companies sought out and used as transshipment points and as false destinations countries with the infrastructural and economic base suitable for transshipment and the operation of foreign companies, but with regulatory environments that turned a blind eye to proliferation activities. The primary example of this was Dubai, within the larger United Arab Emirates.

Third, Iran structured the proliferation network so that the actual acquisition and transport of the goods was commercial and seemingly legitimate up until the last stop before Iran. In most cases, this last stop was the United Arab Emirates, although there were several other jumping off points in Asia.

Fourth, as with all proliferation networks, Iran's brokers hid the true destination of the goods being bought, and the nature of the goods, and obfuscated the nature of the buyers and brokers. Notably, however, Iran made extensive of Iranian nationals and co-ethnic brokers operating outside of Iran, which had advantages and disadvantages for the network.

Fifth, for the final transport segment between Dubai and Iran (it is approximately 260 kilometers between Dubai and the Iranian port of Bandar Abbas), Iran used some amount of

informal trade, relying partly on the informal *dhow* trade that had long moved goods across the Straits of Hormuz, allowing the formal, traceable trade networks to end in Dubai.[28]

Characterizing Iran's networks

As with North Korea, the diagrams for Iran below show how Iran structured its networks to evade scrutiny or interdiction, and to obfuscate the identities of the goods, actors, and end points for the goods.

Figure 5 shows the Iran import networks highlighted by group locations. Iran nodes (firms that are located in Iran) make up 33% of the total. The UAE makes up more than 10% of the nodes in the group location network, despite not being a supplier to Iran (the US and the UK emerge as the main supplier countries for Iran in these networks, largely because they are the main sources of the prosecution data), while China (which is both a supplier country as well as a broker location) makes up 4%, and Turkey and Malaysia make up approximately 2.5% each. The UAE, followed distantly by China, Turkey and Malaysia, thus emerges as the main transshipment point. The descriptions of the transactions themselves (which are generally from summaries of US sanctions and export control prosecutions) tend to end the identified transport chain for prohibited items in the last transshipment point before Iran, whether it is Turkey, the UAE, or Malaysia. The implication, at least for the UAE, is that the freight forwarder in the UAE sent the goods on to Iran, or that the goods were transported informally from the UAE to Iran.

Figure 6 shows the nationalities of the firms involved in the import networks: they are largely the same as in Figure 5. This suggests that the *firms* at least that were operating on behalf of Iran were operating inside the countries where they were based (although in some cases this was because the local firm was the locally incorporated branch of a foreign firm).

However, Figure 7, which shows the nationalities of the individuals involved in the Iran import networks, suggests that, inside of these countries, including both suppliers (the US and the UK), and transshipment points such as the UAE, it is largely individuals who may have non-market ties back to Iranian procurement nodes (such as Iranian co-nationality) who are serving as acquisitions and transport brokers. In Figure 7, at least 44% of the total nodes have Iranian nationality, while UAE nationality makes up 8% of the total, and US nationality makes up 17% of the total (compared to 22% of the total group locations). The difference between

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

UAE and US group location and individual nationality appears to be made up of Iranians (many of whom have direct business ties back to Iran), operating in the UAE and the US. China was the only country besides Iran that increased its share from the group location network to the individual nationality network (from 4% to 5%), suggesting that Chinese nationals were likely to be the only brokers and suppliers working outside their home countries in the Iran network.

There are several distinctives about Iran's networks that can be derived from the figures. First, while non-Iranian brokers existed, the Iran import network between the 1990s and 2018 can be characterized as one in which Iranian buyers liaised with Iranian brokers located in supplier countries or third countries that could serve as bases for acquisitions brokers or as transshipment points for the goods themselves. Thus, while the network appeared to geographically diverse, it was largely a network of Iranians.

Second, where the import networks did use transshipment points for goods (in some cases, the goods or services were shipped directly to Iran, depending on the origin country), Iranian nationals operating as brokers often (perhaps even usually) used the United Arab Emirates, no doubt because it provided three advantages to Iran: a permissive business environment for starting up and running companies, a permissive trading environment (at least prior to 2013), and geographical proximity to Iran. This meant, however, that, while Iran built an extensive network, the network had a chokepoint, both in terms of countries used for brokerage, and the types of individuals involved. This inflexibility was specifically within the Iranian-brokered networks. Where there were third-country national brokers (such as in China, Malaysia, and Turkey), they were also willing and able to route the goods themselves through other countries (although usually through China, Malaysia, and Turkey).

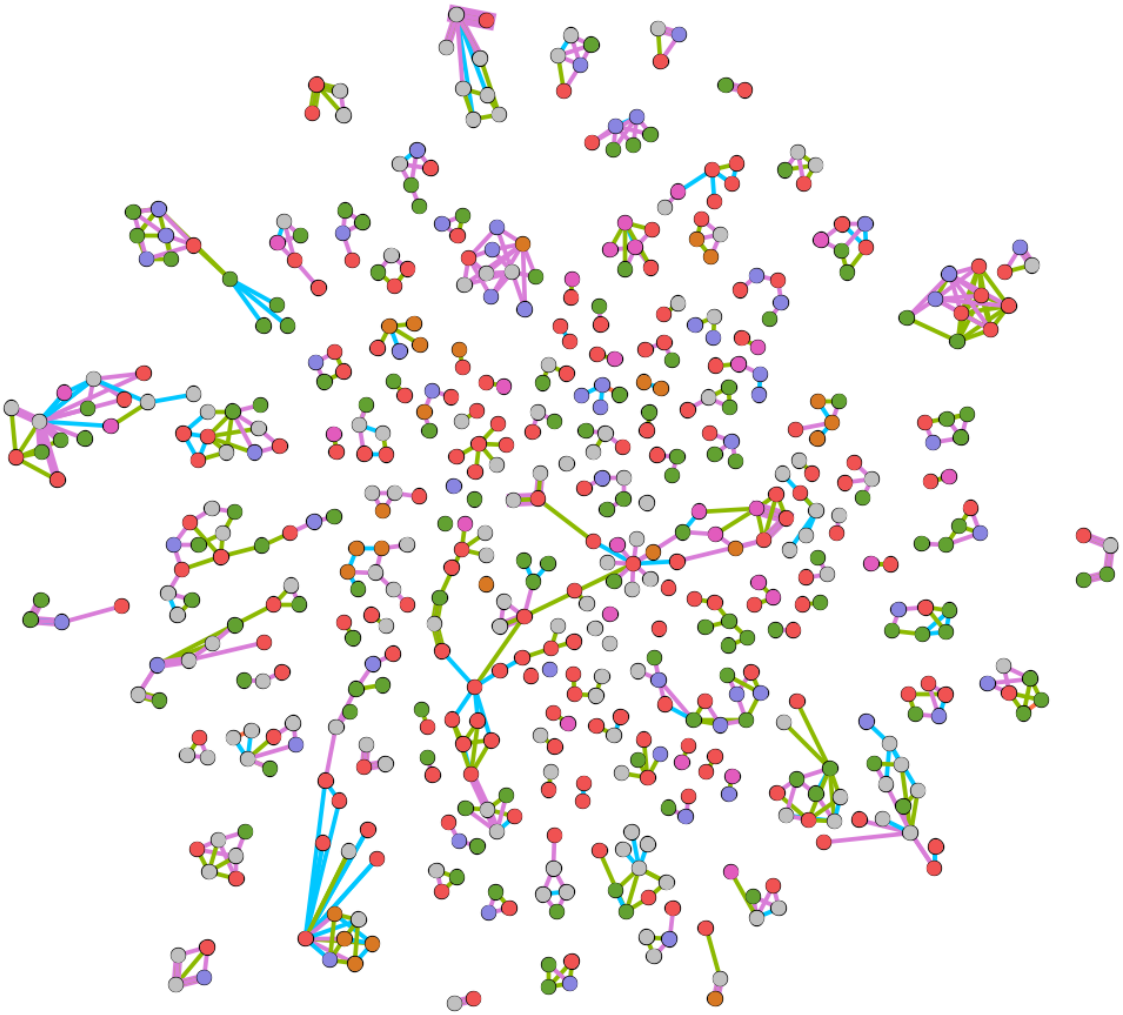

Figure 5. Iran's import networks, with group locations highlighted (Iran = red; United States = green; UAE = purple; China = pink; United Kingdom = orange; others = gray)

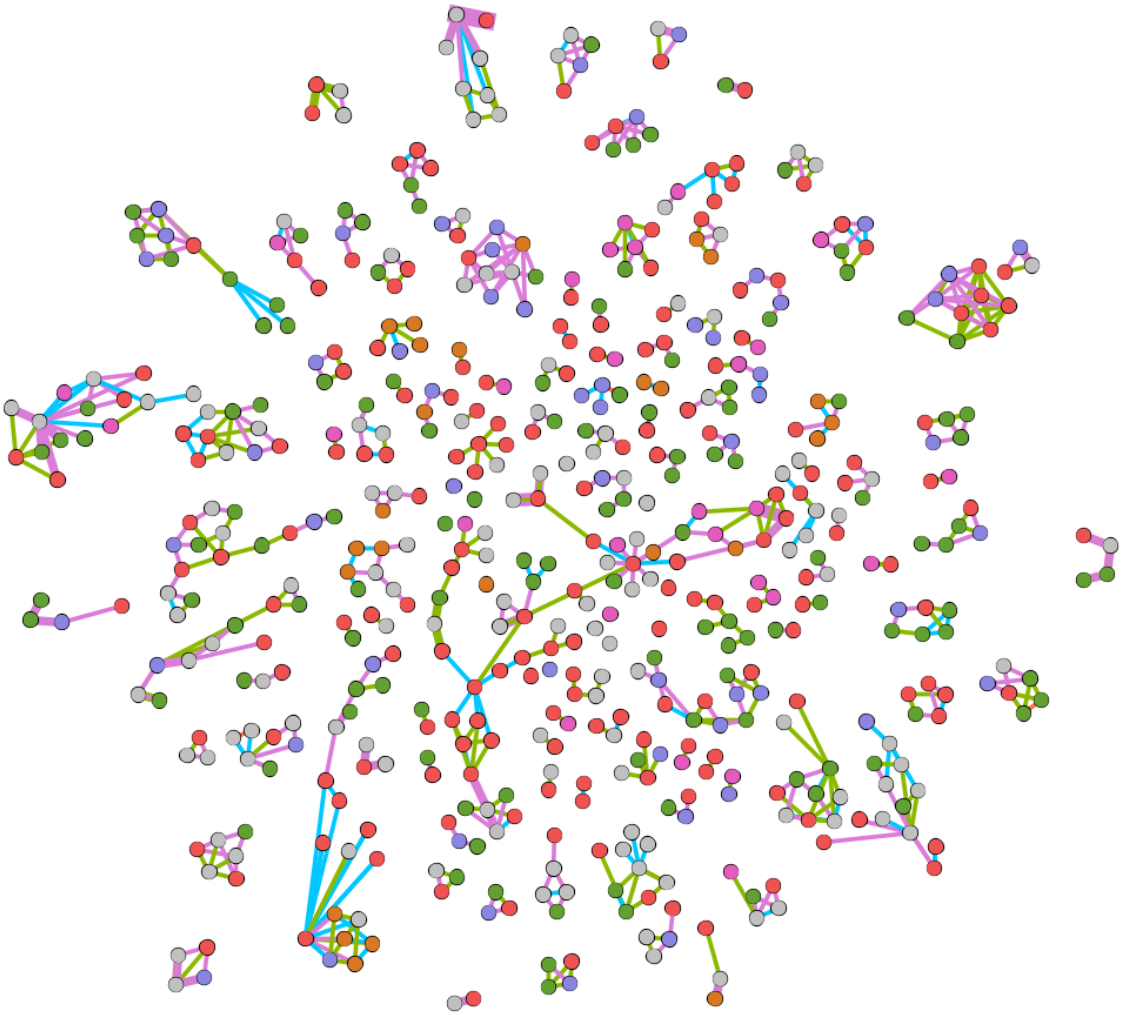

Figure 6. Iran's import networks, with group nationality highlighted

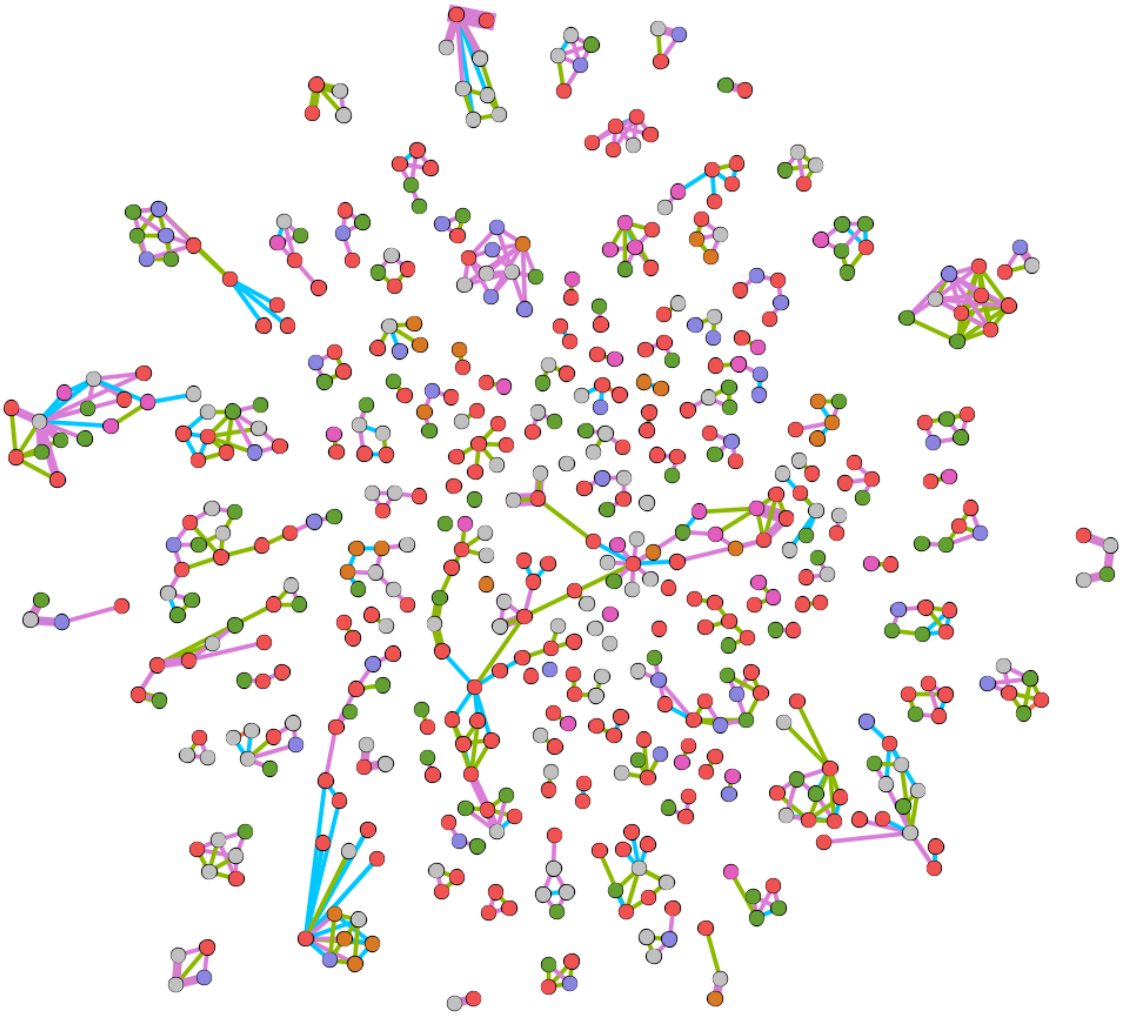

Figure 7. Iran's import, networks, with individual nationality highlighted

The key to Iran's failure

These strategies were not ultimately (as of 2021) successful in actually acquiring a nuclear weapon for Iran, although this is perhaps setting the bar too high. Rather, we can say that, while Iran has not necessarily given up its nuclear ambitions (or at least its ambitions for nuclear latency), despite a program that apparently started as early as the late 1980s, Iran had not been successful in developing a weapons by 2013, when the US eased up on enforcement as a prelude to negotiating the JCPOA, and was having trouble moving the necessary goods for its programs (and other programs) between Iran and the rest of the world.

The main determinant of Iran's failure appears to have been the network's relative inflexibility: at the end of the day, Iran pursued a network with greater security and control at the cost of flexibility. This strategy was effective as long as the nodes, links, routes and methods held. Once these were removed, either by actual removal of the actors involved, or by a change in the policy environment in key countries, Iran had a much harder time. The primary means by which Iran maintained security and control over the acquisitions network was by using Iranian nations and ethnic Iranian citizens of third countries as acquisitions brokers, and even, in some cases, as suppliers. While this minimized defection, and enabled Iran to leverage non-market relationships, it also meant that the brokers were relatively simple to identify once found.

Iran's global location also worked against it, inasmuch as it was denied territorially adjacent countries that were both technologically advanced and politically friendly (or at least ambivalent about enforcing non-proliferation measures) – the most technologically advanced country in the Middle East, Israel, was implacably opposed to the Iranian program, as was the competing regional hegemon, Saudi Arabia. Pakistan (which, perhaps unwittingly, did in fact aid Iran's nuclear program in the 1990s) and Turkey were the two adjacent countries with the relevant technology, but their relations with Iran waxed and waned over the relevant time period, in part due to Sunni-Shiite conflicts, and in part due to varying responsiveness to US pressure to deny Iran technology or trade. As a result, while there were a number of brokers (Iranian and otherwise) who operated out of Turkey, the main country where Iran was able to arbitrage gaps between regulatory focus and capability was the United Arab Emirates, where brokers set up firms (often in the free trade zones of Dubai) to serve as acquisitions and transport brokers in order to tranship proliferation-relevant goods onward to Iran.

Yet Iran made little use of state prerogatives and resources for its inward proliferation network beyond brokering in the UAE, and transporting goods between the UAE and Iran. In practice this meant that the majority of its goods were shipped via commercial routes and methods from suppliers beyond both the UAE and Iran, and transhipped through the UAE, thus leading to a centralized territorial layout for the network, which made it more vulnerable to interdiction.

After the UAE was persuaded to crack down on exports to Iran, and Iranian business operations in the country by 2013, Iran was left with few options for chains that followed commercial routes (as it needed a replacement with similar characteristics to the UAE), and was susceptible to monitoring and hostile policy for state-centered proliferation methods. This lack of flexibility was somewhat mitigated when Iran *did* use third-country acquisitions and

transport brokers – brokers who were either located in countries far afield from the UAE or Iran (although in many cases they still routed the goods through the UAE) or brokers who were neither Iranian nationals nor ethnic Iranians. In these cases, the chains back to Iran demonstrated more flexibility in their choice of routes, methods, and use transshipment points, at a cost (to Iran) of security and control.

IMPLICATIONS

The routes taken, and the brokers used (and their ties with the buyers back in Iran and North Korea), are neither necessary nor sufficient to explain success and failure in nuclear proliferation overall. Just as important in acquiring an actual working bomb is the ability to have a properly functioning research program, and to be able to assimilate and use new technical knowledge.[29] However, the story of Iran and North Korea's procurement networks for banned items (either because of export controls or sanctions) does suggest that different countries might pursue different strategies for pursuing those goods, and in the process create differently structured networks that come with tradeoffs in flexibility, security, and control. North Korea's willingness to trade off security and control for flexibility meant that it solved the problem of evading enforcers by not solving the problem at all: it had other countries solve the problem for it. By contrast, Iran's strategy probably worked more efficiently when it worked (in the sense that Iran could more reliably funnel goods from top-tier supplier countries back to Iran), but was susceptible to being cut off. For policymakers involved in sanctions enforcement and export control regimes, focusing on the supplier countries is only half the battle: just as important are the countries that serve as transport and acquisitions brokerage points, often before they themselves are cognizant of the threat. In addition, it is important in looking at countries of concern to identify the types of networks they are likely to build in their pursuit of banned items. Depending on the nature and spread of their diaspora, the state of their nuclear program, how they are integrated into the global economy, and their risk appetite, the networks may vary significantly from country to country.

[29] Malfrid Braut-Hegghammer, *Unclear Physics: Why Iraq and Libya Failed to Build Nuclear Weapons* (Ithaca and London: Cornell University Press, 2016); Wyn Q Bowen and Christopher Hobbs, "Sensitive Nuclear Information: Challenges and Options for Control," *Strategic Analysis* 38, no. 2 (2014); Jacques EC Hymans, *Achieving Nuclear Ambitions: Scientists, Politicians, and Proliferation* (Cambridge University Press, 2012).