HYBRID NETWORKS AND THE FUTURE OF PROLIFERATION

Justin V. Hastings
University of Sydney

Prepared for the International Studies Association 2019 Annual Meeting, Toronto, Canada, 27-30 March 2019.

Chapter 1 of *A Neophyte's Guide to Proliferation Networks: How They Work and How to Stop Them.*

The days of a state pursuing nuclear weapons using its own state prerogatives and resources are over. Instead, the state must rely on cooperation with private individuals and firms around the world, and form proliferation networks. In this paper, I develop a theory of the structure and behavior of non-state and hybrid state/non-state proliferation networks. I argue that proliferation networks can be thought of as overlapping social and logistical networks for which arranging and then moving technology around the world is not a trivial task. This reliance on non-state actors, particularly as brokers, allows states to acquire, transport, and sell what they want, but introduces vulnerabilities and trade-offs into the networks. Non-state networks that trade in nuclear and illicit materials face the same trade-offs.

Acknowledgments: Research for this book was supported in part by grants from the MacArthur Foundation (#100981) and the Australian Research Council (DP140102098 and FT160100235).

In this chapter, I build a framework to structure our analysis of the challenges proliferation networks face, their strategies to overcomes those challenges, and factors in their success or failure. After developing an economic geographic understanding of proliferation networks as nodes connected by social ties, and the movement of physical goods and information across different countries, I move on to the fundamental challenge for proliferation networks: successfully moving technology and materials through countries that are ambivalent or hostile their activities. This challenge colors how proliferation networks are structured, where they are located, and how they behave. Next, I outline the structure of proliferation networks, and categorize the different actors within the networks as suppliers, buyers, and different types of brokers. Proliferation networks can categorized by the access to state prerogatives and resources that influence how and where they move goods across the globe, as well as the direction of the flow of technology and materials relative to the state of proliferation concern. Finally, I provide a menu of strategies that proliferation networks use, in terms of how they structure themselves, how they move goods around the world, and how they generally attempt to overcome the fundamental challenge of proliferation networks.

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.[1] 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

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

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[2]), and the links between the nodes to be social or treaty relationships, or some other form of cooperation.[3] In his work on proliferation networks, for instance, Alex Montgomery treats entire countries as nodes, between which flow nuclear components and expertise.[4] 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).[5]

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.[6] 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 are being

---

[2] 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).

[3] 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).

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

[5] "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).

[6] 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.

moved from point to point – over what kind of terrain, using what kind of transportation mechanism.[7]

Using an economic geographic approach, we can conceive of proliferation networks as global value chains,[8] 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 characterise 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?

[7] 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).

[8] 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).

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 (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.[9] 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'[10], 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.[11] Nodes involved

[9] 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

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

[11] 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.

in proliferation fall broadly into three categories: suppliers, coordinators (brokers), and buyers.[12] 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 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.[13]

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.

[12] 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).

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

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 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.

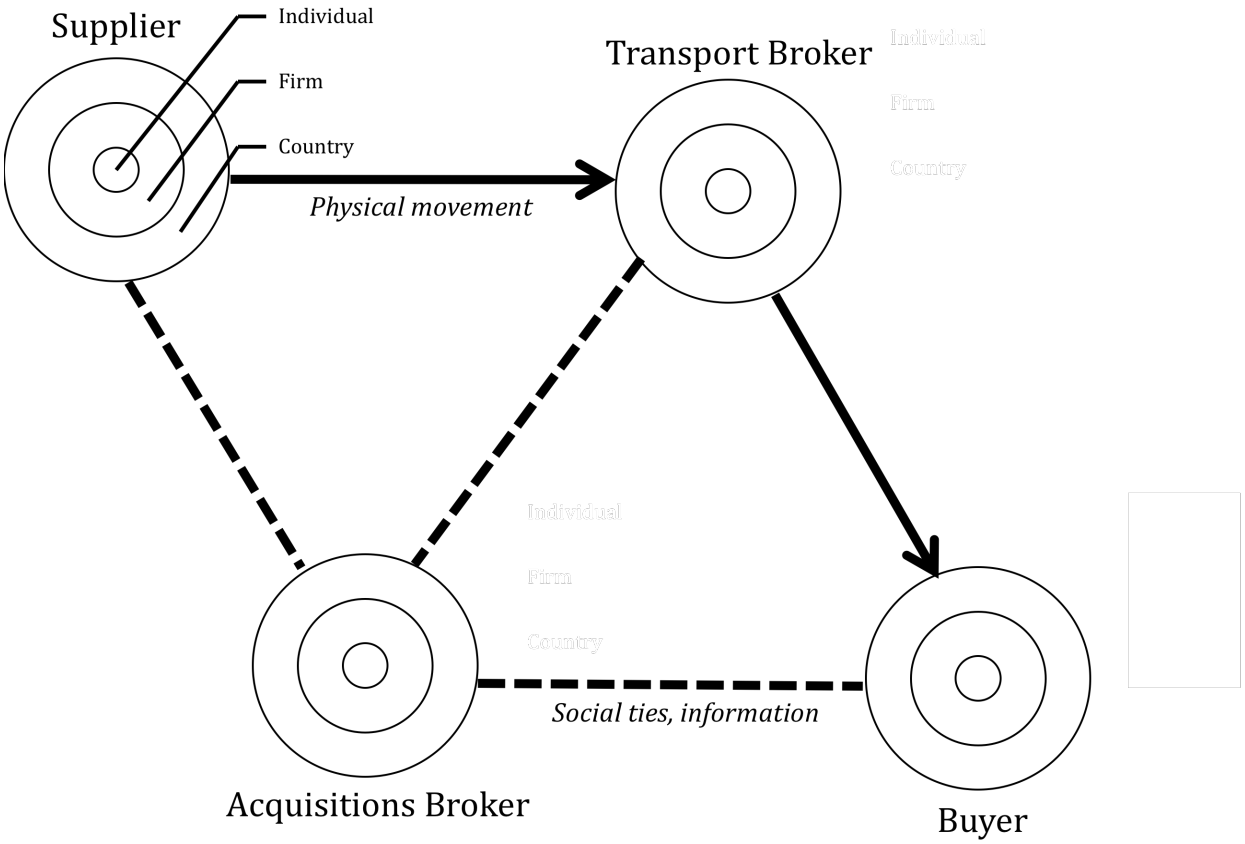
What environments do the network actors face?

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.[14] 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.[15]

Figure 1.1. Conceptual diagram of a proliferation network



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

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.[16] 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 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

[16] 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).

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.[17]

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.[18] The structure of proliferation networks, and the strategies that proliferators use, are a result of how they attempt to resolve these problems.

Types of proliferation networks

The key variable in determining the geographical layout of (and thus the challenges faced by) the proliferation networks created by suppliers, brokers, and buyers, and strategies used by the actors in the networks, is the access that brokers in particular have to state resources. State involvement in proliferation comes not in defining nodes as having state or non-state status (which may be ambiguous, or unknowable in any case), but in assessing the effects that access to state transportation infrastructure, state financial resources, or state diplomatic prerogatives have on the structure of the networks, the location and/or nationality of the nodes, the routes used to transfer goods or knowledge, and the methods employed to move between nodes.[19]

If every actor – supplier, coordinator, and buyer -- is either state or non-state (inasmuch as they avail themselves of state or non-state resources), there are eight permutations of suppliers, coordinators, and brokers in categorizing proliferation networks (see Table 1.1). First, non-state actors (individuals and firms) may knowingly or unknowingly supply a state's weapons program via state coordinators (or more specifically, coordinators with access to state prerogatives and resources). Pakistan's initial nuclear supply network in the 1970s is a

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

[18] 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."

[19] Hastings, "The Geography of Nuclear Proliferation Networks: The Case of Aq Khan." If a state-owned firm is located within the state for which it is proliferating, this can also be taken as a sign of a favorable political and regulatory environment (although there is nothing in principle stopping cooperating non-state firms from enjoying the same environment).

particularly good example of this type of network (as will be discussed in Chapter 2). These networks can bypass commercial routes and transport goods directly back to the buyer country, and run acquisitions brokerage operations that can approach non-state suppliers in a number of countries. At the same time, non-state suppliers in hostile states may not knowingly cooperate with proliferating state brokers and buyers.

Second, private firms or individuals might supply a state's weapons program via non-state coordinators (or more specifically, coordinators without access to state prerogatives and resources). Abdul Qadeer Khan's network to supply Libya (covered in Chapter 2) was arguably an example of this. While this configuration allows for a fair amount of protection from scrutiny, it may require the network to rely on commercial routes and centralize the network in locations where the brokers have both social and transport ties.

Third, states might transfer technology and materials to other states entirely using state resources. In this case, strategic trade controls may not be relevant, since both states bypass other countries' acquisitions and transport coordinators. Many of the sensitive nuclear assistance agreements of the past would fall into this category, as would the apparent North Korean cooperation with Syria in building the nuclear facility that was destroyed by Israel in 2007.[20] These networks are arguably the most difficult to stop, inasmuch as both supplier and buyer are using state prerogative and resources, but are also outside the scope of most facets of the non-proliferation regime (state direct action as Israel's attacks on Iraq and Syria, or interception of state-owned ships on the high seas, such as through the Proliferation Security Initiative, aside).

Fourth, the suppliers, coordinators, and buyers might all be non-state actors, relying wholly on commercial or smuggling networks with no benefit from state assistance or resources. The networks that traffic in radioactive sources and small quantities of nuclear materials would be apt examples of this type of network.[21] These networks are fully at the mercy of commercial infrastructure, or smuggling networks, and as such may be able to escape scrutiny through maintaining tight social ties and other typical criminal strategies, they are also unlikely to be able

[20] Wyn Q Bowen and Christopher Hobbs, "Sensitive Nuclear Information: Challenges and Options for Control," *Strategic Analysis* 38, no. 2 (2014); Matthew Kroenig, "Importing the Bomb: Sensitive Nuclear Assistance and Nuclear Proliferation," *Journal of Conflict Resolution* 53, no. 2 (April 2009); "Exporting the Bomb: Why States Provide Sensitive Nuclear Assistance," *American Political Science Review* 103, no. 1 (February 2009).

[21] Kupatadze, "Organized Crime and the Trafficking of Radiological Materials: The Case of Georgia."; Justin V. Hastings, Adam N. Stulberg, and Philip Baxter, "Technology, Materials, and Knowledge Transfer in Nuclear Proliferation Networks: Findings and Implications," (Sydney: University of Sydney, 2015).

to move more than small quantities of technology or materials, and the buyers themselves may not be equipped to use the goods even if they do arrive safely.

Fifth, states may supply other states with technology and materials using non-state acquisitions and (particularly) transport brokers. North Korean exports of weapons and other technology to African and Middle Eastern countries (covered in Chapter 5) arguably fall into this category. While the networks do not have to resolve the problem of getting into or out of the supplier or buyer country, they must move goods via commercial routes and methods between two states are likely to be under external scrutiny, and at both the start and finish of the supply chain, the suppliers and brokers must find ways to obfuscate the origin, destination, or the nature of the goods to the transport brokers, and in some cases the acquisitions brokers.

Finally, state suppliers providing technology or materials to non-state actors via state or non-state coordinators is unlikely, but conceivable if a state for some reason decided to provide missiles or weapons or mass destruction to a terrorist group or insurgency.[22] Arguably Iran's provision of missiles to the Houthis in Yemen during the conflict there falls into this category.[23] While, assuming the state use its own transportation and coordinator resources, the goods are likely to arrive with the non-state actor (assuming the network can solve the problem of getting the goods into the 'buyer' country), the deniability of the actions by the supplier state is relatively low, so it is likely that states will demur unless the risks are low (as appears to be the case of the Houthis, where *Qatar* arguably suffered the greatest cost for Iran's actions).

Table 1.1. Categories of likely proliferation networks

Supplier	Coordinator	Buyer	Example
Non-state	State	State	Pakistan's nuclear weapons program
Non-state	Non-state	State	Libya's nuclear weapons program
State	State	State	North Korea-Syria nuclear cooperation
Non-state	Non-state	Non-state	Radioactive source and nuclear materials trafficking
State	Non-state	State	North Korean exports to African, Middle

[22] The final combination – non-state actors providing technology or materials to other non-state actors via a state coordinator – seems like a high-risk, low-benefit activity for the putatively involved state, and is unlikely to be observed in nature.
[23] Michelle Nichols, "Parts of Missiles Fired at Saudi Arabia Came from Iran: U.N. Chief," *Reuters* 15 June 2018.

			Eastern countries
State	State	Non-state	Iranian supply of missiles to Houthis in Yemen

The direction of proliferation networks

Across the different permutations of suppliers, coordinators, and buyers are three types of networks in which the state might be (or might not be) enmeshed, as determined by the direction of the flow of technology or materials relative to the state of proliferation concern.

Inward proliferation

First, the state of proliferation concern might be the ultimate buyer of the technology or materials. In this network, the supply chain ends inside the state of proliferation network, so the main challenge for the proliferator is to obscure the ultimate destination of the technology or material (which is otherwise totally legitimate), and to move the goods over the 'final mile,' the border between the state and its firms, and the rest of the world.

Outward proliferation

Second, the state of proliferation concern might be the initial supplier of the technology or materials. In this network, the supply chain begins inside the state of proliferation concern. While it would not necessarily be a challenge to export the technology or materials from the proliferating state, the main task of the proliferator would be to conceal the provenance of the goods through the entire supply chain to the destination. Assuming another state is a buyer, the 'final mile' may not be a problem for the network, but concealing the provenance might be difficult, in no small part because a buyer state acquiring technology or materials through a proliferation network is likely to be under surveillance or export control scrutiny nearly to the same extent as the supplier state.

Brokerage networks

Third, the state of proliferation concern might be neither the ultimate buyer nor seller, but use its state prerogatives and resources, or provide political cover for other actors, to serve as an acquisitions or (more rarely) transport broker for technology or materials. This type of network is

especially difficult for counter-proliferators to detect, since neither the provenance nor the destination of the goods are necessarily problematic or questionable, and the proliferator's main involvement comes in facilitating transfers, which could allow even more arms-length involvement than would be the case for inward or outward proliferation networks. With that said, as we will see, the state of proliferation concern is likely to use methods in serving as a brokers for two third-parties that are similar to those it uses for its inward and/or outward proliferation networks.

Proliferation network strategies

Depending on the type of proliferation network, and the direction of proliferation, 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 surveill, 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).[24]

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.[25]

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.

Use of state prerogatives and resources

For a proliferating state supplier, broker, or buyer, using state prerorgatives and resources theoretically seems like the most straightforward approach to proliferation: the state can achieve

[24] 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).

[25] 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).

maximum security within the network (since the nodes are controlled by the state), and presume a minimum of interference from other states that comes with diplomatic status (up to a point). Entering the buyer country, or exiting the supplier country, assuming the state is supportive of the transaction, is no longer a problem. Moving goods on state-owned ships or airplanes also allows the network to bypass commercial routes and chokepoints that could be controlled by hostile states. Arranging transactions using state brokers located in diplomatic or state-controlled outposts maximizes control over the network, and likewise minimizes the need to bring in possibly unreliable third-parties or rely on commercial means of arranging deals.

Extensive reliance on state prerogatives and resources has impliactions for the territorial layout of a proliferation networks. State resources would lead to a more decentralized series of routes, where proliferation goods could use a variety of routes to get from the supplier to the buyer, making it more difficult for hostile states to stop all flows. The territorial layout of these networks thus tends to be either direct between two proliferating states (if they are transporting materials themselves directly), thus bypassing commercial infrastructure (and other countries' ability to interdict them) and unfriendly countries or, if there are multiple suppliers, territorially dispersed routes between suppliers and the buyers.

But there are costs. The states that are likely to be using their own resources to power the logistical networks undergirding proliferation do not have an unlimited number of diplomatic outposts or state-owned ships and planes, and they are often geographically concentrated within countries with whom the proliferating state has relations. Acquisitions or transport brokers that are operating out of diplomatic missions are limited to wherever the state has outposts. The use of state resources can itself draw scrutiny from other states, meaning that a state's limited resources can be tracked and surveilled by hostile states with sufficient attention and resources – there are not an infinite number of North Korea-owned cargo ships or diplomatic outposts. Moreover, while state officials acting as brokers can operate with diplomatic immunity and/or financial resources that might only be available to state companies, they are also the actors most likely to be subject to scrutiny by intelligence services (and with the least amount of plausible deniability), and the most likely to attract attention when dealing with non-state suppliers who need to apply for permissions related to strategic trade controls.

The failure points of networks using state prerogatives and resources are clear. The closure of diplomatic outposts, the expulsion of diplomatic and state-run companies from

territories, and the denial of international resources to state-owned transport can several cramp the ability of proliferation networks to operate. Sanctions against state-operated companies and individuals raises the cost of foreign companies and individuals dealing with the proliferating states, and in many cases can cut off their relationships entirely. Even for the links that are not cut off,

Non-state strategies

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 other 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.[26] 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 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

[26] 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).

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.

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 *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 indivudals. 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.

Informal trade

Proliferation networks may also engage in informal trade, where actors (whether individuals or registered companies) bypass trade regulations and/or checkpoints when trading what are otherwise legal goods.[27] Nearly all activities of proliferation networks involve partially bypassing regulations (such as mis-declaring the final user or the nature of the goods being traded), but proliferation networks can also simply fully bypass trade regulations and physical checkpoints.

The peculiar problem of proliferation networks is that, because much of the technology that goes into missile and nuclear weapons (for instance) has genuine industrial uses, states are often attempting to regulate the use, importation, and exportation of technology and material without banning them outright (unlike, for example, drugs and guns). Many technologies and materials only become 'illicit' upon being tied to a specific supplier, buyer, or broker. As a result, for proliferation networks it is a matter of how far along the chain they can maintain the licit nature of the goods, and at what point in the supply chain they may find it useful to switch to informal trade.

In some instances, suppliers and brokers may simply ship goods through normal channels without seeking or receiving export or shipping permits. This is made easier when the supplier

[27] Caroline Lesser and Evdokia Moisé-Leeman, "Informal Cross-Border Trade and Trade Facilitation Reform in Sub-Saharan Africa," in *OECD Trade Policy Working Paper Series* (Paris: Organization for Economic Co-Operation and Development, 2009).

state or broker state either does not have a regulatory structure in place or does not consider the goods (for various reasons) to have been imported, exported, or transshipped through the country.

In other cases, suppliers, brokers, and buyers may physically bypass the checkpoints, and avoid any interaction with trade regulations. This has the advantage of shifting the transaction from a matter of trade regulation (where a hostile state may be capable) to border security and intelligence (where a hostile state may not be so capable), and more generally relieves proliferation networks of the need to use other strategies (in particular obfuscation) which rely on deceiving authorities into thinking a particular transaction is legitimate.

Yet informal trade comes with a host of risks. Because, in the course of bypassing formal checkpoints and regulations where state scrutiny is concentrated, the network is not using the standard commercial transportation infrastructure, it must either supply its own means of transport or it must rely on routes and methods that do not benefit from the technologies of globalization that exist at commercial hubs, thus increasing the cost and time needed to move proliferation goods.[28] Because the network needs to avoid areas where state attention is high (such as airports or seaports), it is limited to traversing terrain that is often physically difficult to cross. If it does not have its own long-distance transport infrastructure, the network is also limited to relatively short distances, between adjacent countries. In addition, it must build up social ties – other smugglers, border guards, officials willing to look the other way -- that allow it to cross border outside the standard checkpoints. Building up these social ties requires time and money, just as partially bypassing regulations while using formal trade infrastructure does.[29]

For states, or at least for proliferation networks that have set supplier or buyer countries (such that the beginning or endpoint is essentially immovable – Iran has little interest in dual-use goods for its nuclear program ending up anywhere else but Iran), because it must avoid state-controlled chokepoints and globalized infrastructure, informal trade is really only useful at the beginning or end of the chain.

Concealing proliferation-relevant materials in shipments of legitimate goods can also bring difficulties if an involved state, firm, or individual is sanctioned, and the proliferation network loses the ability to ship the legitimate goods or use the 'legitimate' firms for transport.

[28] Hastings, *No Man's Land: Globalization, Territory, and Clandestine Groups in Southeast Asia*.
[29] Justin V. Hastings and Yaohui Wang, "Informal Trade Along the China-North Korea Border," *Journal of East Asian Studies* (2018).

Market exit by firms due to sanctions (either because they are directly forced out of the market, or because their main imports, exports, and investments are rendered unprofitable by sanctions and their enforcement) can decrease the pathways available for informal trade networks to move goods down the chain.

Finally, except for goods that are sold in gray markets, such as North Korea's border markets selling consumer goods from China[30] -- and dual-use technological items and nuclear materials are unlikely to be sold in such markets -- informal trade is not by and large amenable to market relationships., or to unwitting third-party transport or acquisitions brokers at the point of smuggling. Increased border security by adjacent countries and the destruction of the social networks that undergird informal trade impose high costs on informal traders, as they must take invest time and money in building a new social network, in addition to the security loss that defecting actors might impose on the proliferator.

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 perhap 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

[30] Hyung-min Joo, "Hidden Transcripts in Marketplaces: Politicized Discourses in the North Korean Shadow Economy," *The Pacific Review* 27, no. 1 (2014); Andrei Lankov and Seok-hyang Kim, "North Korean Market Vendors: The Rise of Grassroots Capitalists in a Post-Stalinist Society," *Pacific Affairs* 81, no. 1 (Spring 2008).

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.

References

Baxter, Philip, 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.

Bowen, Wyn Q, and Christopher Hobbs. "Sensitive Nuclear Information: Challenges and Options for Control." *Strategic Analysis* 38, no. 2 (2014): 217-29.

Corera, Gordon. *Shopping for Bombs.* Oxford: Oxford University Press, 2006.

Cronin, Audrey Kurth. "Behind the Curve: Globalization and International Terrorism." *International Security* 27, no. 3 (Winter 2002-2003): 30-58.

Cutter, Susan L., Douglas B. Richardson, and Thomas J. Wilbanks, eds. *The Geographical Dimensions of Terrorism*. New York: Routledge, 2003.

Dicken, P., P. F. Kelly, K. Olds, and H. W.-C. Yeung. "Chains and Networks, Territories and Scales: Towards a Relational Framework for Analyzing the Global Economy." *Global Networks* 1, no. 2 (2001): 89-112.

Flint, Colin. "Terrorism and Counterterrorism: Geographic Research Questions and Agendas." *The Professional Geographer* 55, no. 2 (May 2003): 161-69.

Frantz, Douglas, and Catherine Collins. *The Nuclear Jihadist.* New York: Twelve, 2007.

Gereffi, Gary, and Karina Fernandez-Stark. "Global Value Chain Analysis: A Primer." Durham, NC: Center on Globalization, Governance & Competitiveness (CGGC), Duke University, 2011.

Gereffi, Gary, John Humphrey, and Timothy Sturgeon. "The Governance of Global Value Chains." *Review of International Political Economy* 12, no. 1 (2005): 78-104.

Gereffi, Gary, and Miguel Korzeniewicz. *Commodity Chains and Global Capitalism.* Westport, CT: Praeger, 1994.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. "Network Analysis in International Relations." *International Organization* 63 (Summer 2009): 559-92.

HARMONY. "Al-Qaida's (Mis)Adventures in the Horn of Africa." West Point, NY: Combating Terrorism Center, United States Military Academy, 2007.

Hastings, Justin V. "Geographies of State Failure and Sophistication in Maritime Piracy Hijackings." *Political Geography* 28, no. 4 (May 2009): 213-23.

———. "The Geography of Nuclear Proliferation Networks: The Case of Aq Khan." *Nonproliferation Review* 19, no. 3 (September 2012): 429-50.

———. *No Man's Land: Globalization, Territory, and Clandestine Groups in Southeast Asia.* Ithaca and London: Cornell University Press, 2010.

Hastings, Justin V., Adam N. Stulberg, and Philip Baxter. "Technology, Materials, and Knowledge Transfer in Nuclear Proliferation Networks: Findings and Implications." Sydney: University of Sydney, 2015.

Hastings, Justin V., and Yaohui Wang. "Informal Trade Along the China-North Korea Border." *Journal of East Asian Studies* (2018).

Henderson, Jeffrey, Peter Dicken, Martin Hess, Neil Coe, and Henry Wai-Chung Yeung. "Global Production Networks and the Analysis of Economic Development." *Review of International Political Economy* 9, no. 3 (August 2002): 436-46.

Hinderstein, David L. Albright and Corey. "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, FL, 2 July 2004.

Joo, Hyung-min. "Hidden Transcripts in Marketplaces: Politicized Discourses in the North Korean Shadow Economy." *The Pacific Review* 27, no. 1 (2015/04/20 2014): 49-71.

Keck, Margaret E., and Kathryn Sikkink. *Activists Beyond Borders: Transnational Advocacy Networks in International Polictics.* Ithaca, NY: Cornell University Press, 1998.

Kenney, Michael. *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*, edited by Miles Kahler, 79-102. Ithaca: Cornell University Press, 2009.

Krebs, Valdis. "Uncloaking Terrorist Networks." *First Monday*, no. Vol. 7, No. 4 (April 2002).

Kroenig, Matthew. "Exporting the Bomb: Why States Provide Sensitive Nuclear Assistance." *American Political Science Review* 103, no. 1 (February 2009).

———. "Importing the Bomb: Sensitive Nuclear Assistance and Nuclear Proliferation." *Journal of Conflict Resolution* 53, no. 2 (April 2009): 161-80.

Kupatadze, Alexander. "Organized Crime and the Trafficking of Radiological Materials: The Case of Georgia." *Nonproliferation Review* 17, no. 2 (July 2010): 219-34.

Lankov, Andrei, and Seok-hyang Kim. "North Korean Market Vendors: The Rise of Grassroots Capitalists in a Post-Stalinist Society." *Pacific Affairs* 81, no. 1 (Spring 2008): 53-72.
Lesser, Caroline, and Evdokia Moisé-Leeman. "Informal Cross-Border Trade and Trade Facilitation Reform in Sub-Saharan Africa." In *OECD Trade Policy Working Paper Series*. Paris: Organization for Economic Co-Operation and Development, 2009.
Lutes, Charles D. "New Players on the Scene: A.Q. Khan and the Nuclear Black Market." *Foreign Policy Agenda* (March 2005).
MacKenzie, Donald, and Graham Spinardi. "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons." *American Journal of Sociology* 101, no. 1 (July 1995): 44-99.
Magouirk, Justin, Scott Atran, and Marc Sageman. "Connecting Terrorist Networks." *Studies in Conflict and Terrorism* 31 (2008): 1-16.
Montgomery, Alexander H. "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network." *International Security* 30, no. 2 (Fall 2005): 153-87.
———. "Stop Helping Me: When Nuclear Assistance Impedes Nuclear Programs." In *The Nuclear Renaissance and International Security*, edited by Adam N. Stulberg and Matthew Fuhrmann, 177-202. Stanford, CA: Stanford University Press, 2013.
Nichols, Michelle. "Parts of Missiles Fired at Saudi Arabia Came from Iran: U.N. Chief." *Reuters*, 15 June 2018.
Piazza, James A. "Incubators of Terror: Do Failed and Failing States Promote Transnational Terrorism?". *International Studies Quarterly* 52, no. 3 (2008): 469-88.
Prosser, Andrew. "Nuclear Trafficking Routes: Dangerous Trends in Southern Asia." Washington, DC: Center for Defense Information, 22 November 2004.
Rabasa, Angel, Steven Boraz, Peter Chalk, Kim Cragin, Theodore W. Karasik, Jennifer D. P. Moroney, Kevin A. O'Brien, and John E. Peters. "Ungoverned Territories: Understanding and Reducing Terrorism Risks." Santa Monica, CA: RAND, 2007.
Sageman, Marc. *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press, 2004.
Shapiro, Jacob N. *The Terrorist's Dilemma: Managing Violent Covert Organizations.* Princeton, NJ: Princeton University Press, 2013.
Shapiro, Jacob N., and David A. Siegel. "Underfunding in Terrorist Organizations." *International Studies Quarterly* 51 (2007): 405-29.
Zaitseva, Lyudmila. "Organized Crime, Terrorism and Nuclear Trafficking." *Strategic Insights* 6, no. 5 (August 2007).
Zaitseva, Lyudmila, and Kevin Hand. "Nuclear Smuggling Chains: Suppliers, Intermediaries, and End-Users." *American Behavioral Scientist* 46, no. 6 (February 2003): 822-44.
Zaitseva, Lyudmila, 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.