Oxford Handbooks Online

Arms Supply and Proliferation Networks

David Kinsella and Alexander H. Montgomery

The Oxford Handbook of Political Networks
Edited by Jennifer Nicoll Victor, Alexander H. Montgomery, and Mark Lubell

Subject: Political Science, Comparative Politics, Political Methodology
Online Publication Date: Aug 2016 DOI: 10.1093/oxfordhb/9780190228217.013.33

Abstract and Keywords

Network analyses of global and regional arms flows (including small arms and light weapons, major conventional weapons, and weapons of mass destruction) and related international insecurity and criminality have so far been limited. Yet the literature contains hypotheses that could be explored or tested using network analysis. This chapter discusses supply and demand effects, structural tradeoffs between security and efficiency, pressures to become more or less centralized, and the effects of geography and other network layers. It concludes by reviewing existing data sets and analyses and gauges the potential for network analysis to inform the study of arms transfer networks. Given the general import of these networks for both security studies and policy, there should be a renaissance in the study of arms supply and proliferation networks.

Keywords: weapons of mass destruction, proliferation networks, small arms and light weapons, major conventional weapons, illicit arms trade

Introduction

The transfer of small arms and light weapons (SALW), major conventional weapons (MCW), and weapons of mass destruction (WMD)—as well as the components used in their production—remains a central scholarly focus in the field of security studies and a pressing matter for policymakers and political activists.[1] Despite this, network-analytic approaches to arms transfers are surprisingly infrequent. Network language and imagery are frequently invoked by those who investigate the transfer of weapons and related contraband, but neither social network theory nor the tools of social network analysis (SNA) presently feature prominently in the literature. Yet questions pertaining to global and regional arms flows, proliferation of WMD, and the related matters of international insecurity and criminality should lend themselves quite well to this mode of analysis.

Although network analytic methods are now widely used in political science, some of the main challenges for their application to these questions derive from the limited availability of data. Information on the mostly legal interstate trade in MCW is well developed. But data are often missing or distorted for the trafficking of SALW and WMD, which are restricted in interstate commerce by law or policy.[2] Naturally, clandestine networks of actors (both individuals and organizational entities) are defining characteristics of much of this weapons flow, which also means that their activities and connections are not easy to trace. Describing even the structural features of these networks is therefore a significant challenge.

Nonetheless, the extant literature contains a number of implicit or explicit hypotheses that could be explored or tested using network analysis. Claims that clandestine actors use network forms of organization, for example, have observable implications for the network structures of arms transfers. Similarly, arguments that social or cultural networks facilitate illicit transfers can be tested by comparing these underlying structures with actual arms networks. Hypotheses that brokerage positions are particularly valuable should be reflected in the behavior of middlemen seeking to maintain or expand their influence by preventing competing intermediaries from closing structural holes. And network structures should reflect the varying hostility of the legal and political environment as well as the technical requirements for transfers.

This chapter first provides an overview of the main factors shaping these networks through supply and demand, examining the illicit and/or clandestine nature of many of these ties and the immense variance across levels of analysis and technologies in the arms trade. It then discusses these networks' structural characteristics, focusing on the trade-offs between security and efficiency embodied in them, the pressures on networks to adopt more or less centralized forms, and how different layers in networks relate to each other and adapt to different constraints such as geography. Finally, it reviews some existing data sets and network analyses (surprisingly few at present) and concludes with a discussion of the potential for network analysis to inform the study of arms transfer networks.

Supply and Demand

The analysis of supply and demand factors for arms transfers tends to start with monadic and dyadic considerations rather than network ones. Nevertheless, these considerations hint at possible network mechanisms. Weapons and military-technology transfers ought to be understood as both economic and political transactions; consequently, there should be correlations between economic and political networks. State-sanctioned transfers,

especially those involving MCW systems, are often elements in an ongoing political-military relationship between governments. They are undertaken for the purpose of enhancing the military capability of the receiving state, but they may also afford the supplier some degree of political influence over the recipient (although frequently less than expected) and signal to third parties that the supplier has some interest in the military security of the recipient. When the “political content” of weapons transfers is low—for example, when they are not accompanied by any security commitment by the supplier—they more closely resemble other types of economic transactions taking place on the open market. Governments that allow arms producers within their jurisdictions to export their goods primarily as a means of achieving economies of scale may have little interest in the security implications for receiving states. The same is true for governments selling surplus weaponry after a military demobilization. Nonetheless, even ordinary economic transactions are strongly influenced by network mechanisms (Ward, Ahlquist, and Rozenas, 2013; Ward and Hoff, 2007), and so consequently we should expect even purely economic arms transfers to be influenced by them as well.

The types of weapons and military technology that states are willing to transfer to other states suggest something about the relative political versus economic content of those transactions. Broadly speaking, the political content of SALW transfers is lower than MCW transfers. They do not entail the transfer of high levels of military capability and need not represent a significant measure of commitment by the supplier to the recipient’s security. At the other end of the spectrum, a state is unlikely to be willing to transfer (or assist in the development of) ballistic missiles, antimissile systems, or WMD—international law notwithstanding—in the absence of a close political-military relationship with the recipient. Moreover, these types of transfers take place in a context of broader political deterrence and signaling networks (Spindel, 2015). The security interests of supplier states, therefore, regulate the extent to which global weapons flows are governed by market mechanisms, political forces, or various mixtures of the two. Many of the relevant political relationships are themselves networks, formal military alliances being the most obvious.

On the demand side, both state and nonstate entities seek weapons for an admixture of functional and symbolic reasons. Security demands are frequently the most obviously apparent motive for seeking weapons, but even these can vary depending on the weapons seeker’s particular strategies and repertoires for using violence—which in turn can depend on broader political network positions. The explicit or implicit security ties to the weapons source may be as or more important than the weapons themselves. Other prominent political motivations include seeking prestige through the purchase (or manufacture) of symbolically important weapons or satisfying important internal or external constituencies (Eyre and Suchman, 1996; Kinsella and Chima, 2001; Suchman

and Eyre, 1992). Prestige seeking often occurs when there is a gap between actual network position and aspirational status; diplomatic (and other) networks are central to determining the prestige of states (Kinne, 2014). Finally, weapons transfers can also be shaped by internal organizational competition for resources, such as interservice rivalries in militaries with independent branches (Buzan and Herring, 1998).

Illegal Weaponry and Networks

Illicit weapons networks materialize for fairly obvious reasons. Because global markets for weaponry do not operate freely, but are constrained by states' foreign policies and laws, some of the demand for weaponry is met by means beyond the reach of states. Black and grey markets, for weapons or anything else, form when supply and demand are sufficient to sustain profitable exchange among a collection of actors despite the risks. As in legal markets, exchange will occur when the costs of participating in the illegal market are offset by the net gains from the exchange. But the transaction costs associated with illegal market exchange are invariably higher than in legal markets—although anyone familiar with legal weapons procurement will know that it only vaguely resembles an actual market. There is a premium on information about availability, price, quality, and other matters when goods must be traded out of sight because their exchange runs counter to policy or is prohibited by law. Likewise, the costs of bargaining and sustaining agreements are higher because transactions are extralegal and therefore risky; the parties to the exchange cannot turn to state authorities for purposes of enforcing property rights and contract terms. Add to this the risk of penalty for participating in prohibited exchange and (for some) the accompanying moral costs. Yet for many goods and services, in many places, illegal markets thrive.

Although it is certainly the case that governments and weapons firms are sometimes counted among the actors participating in illicit transactions, this is often attributable to rogue individuals or entities within those organizations. Formal governmental and business organizations structured as hierarchies are not very well suited to achieve the efficiencies necessary to offset the additional transaction costs associated with exchange in illicit markets. This is because they come under the scrutiny of public policy and law, which is anathema to the functioning of illegal markets. Less formal organizations with core-periphery or cell network structures are better able to avoid this sort of scrutiny and to adapt when their illicit transactions are, or may be, exposed. Consequently, we should see illicit arms and proliferation networks adopt these types of structures.

The implications of network theory go beyond the structures adopted by these organizations. Social networks are important to those engaged in activities that must remain underground and unregulated by legal contracts and other mechanisms that

attach to open market exchange. Family ties, personal friendships, and networks that are formed based on sets of common practices, such as shared ethnicity and religion, can give rise to interpersonal loyalties and the trust that reduce transaction costs when the formal rule of law is unavailable. This sort of social capital is obviously not absent from commerce in open markets, but it becomes rather more essential to the movement of illicit or clandestine goods and services by means of a multiplex of crosscutting connections (Kleemans and Van De Bunt, 1999; Lampe and Johansen, 2004; Murji, 2007; Parkinson, 2013). If nothing else, suppliers, traffickers, and consumers must instill confidence among themselves that they share a commitment to keeping the joint enterprise hidden from scrutiny by the agencies of government. About the illicit arms trade, Naylor (2004, 129) notes that “discretion is a proverb, not only with respect to one’s own business but with respect to everyone else’s as well. By an unwritten code, gunrunners, however anxious to cut each other’s commercial throats, rarely rat out each other the way drug dealers routinely do.”

Weapons Network Structures

Although at first glance organizations that are illicit and/or clandestine would seem likely to adopt different network structures than those that are not, network theory is not deterministic about alternative structures. Indeed, it recognizes both that these two characteristics may push in different directions and that organizations face a trade-off between efficiency and security in structuring their networks to accomplish their goals.

It is important to distinguish between these two characteristics—the illegal and the concealed—since they place different structural pressures on networks and produce different behavioral characteristics. They are often lumped together under the term “dark networks.” Consequently, this term runs the gamut from well-developed militant political organizations carrying out insurgencies to criminal networks trafficking in various forms of contraband. It can apply to networks within or between organizations that have goals, use means, or conduct transactions that are illicit or clandestine (although the former frequently requires some of the latter).

Small arms and light weapons transfer networks and WMD proliferation networks tend to be both illicit and clandestine, but not in equal amounts. They both facilitate the diffusion of contraband weaponry. For SALW, this is often (but not always) for the benefit of nonstate actors hostile to states; for WMD, the beneficiaries are typically “rogue states” confronting constraints imposed by the most dominant states in the international community. Law enforcement and national security policymakers, in particular, have been interested in understanding the features of illicit networks that allow them to adapt

to a changing environment. This includes efforts by police and military forces to defeat their activities and dismantle their organizations. Scholarship in sociology, economics, criminology, and political science is contributing to this understanding and providing a set of analytical tools to describe these networks' resiliencies and vulnerabilities (Bakker, Raab, and Milward, 2012; Enders and Su, 2007; Hämmerli, Gattiker, and Weyermann, 2006; Klerks, 2001; Koschade, 2006; Milward and Raab, 2006; Perliger and Pedahzur, 2011; Raab and Milward, 2003; Sageman, 2004). However, at least in political contexts, some analysts caution that the unreflective use of network analysis to identify and target purported vulnerabilities may be ultimately counterproductive (see, e.g., Mac Ginty, 2010).

The Efficiency/Security Trade-off

Illicit networks typically face a trade-off between efficiency and security (see, e.g., Lindelauf, Borm, and Hamers, 2009), although those operating in permissive environments or otherwise taking advantage of ungoverned spaces are less constrained. As previously discussed, organizations that rely on a multiplex of network ties allow members to overcome barriers to collective action—the production and distribution of weapons, gas centrifuges, drugs, and so forth—thereby generating collective as well as private gains for participants. But these networks typically operate in risky environments, and participants must be attentive to their exposure to external threats. Internally, trust and mutual commitment to a financially and/or politically profitable covert enterprise may be enough to maintain the concealment necessary for network security. And when it is not, the threat of violence may suffice.

A trade-off between efficiency and security exists because active networks are more likely to become exposed and fall victim to the disruptive efforts of military and law enforcement authorities. Illicit networks might generally be thought to prioritize security over efficiency, but Morselli et al. (2007, 145) suggest that this is the case only for networks with particular types of objectives:

> When the objective involves a monetary outcome, action in the criminal enterprise context is more limited in terms of time because participants expect a pay-off for their involvement in the network, and as a result, action must be played out within a reasonably short time frame. When the objective is political, time is a more extensive resource and action may be prolonged—the political cause is prioritized over any episodic action and, as a result, a network may lay low and wait for the right moment to act.

One implication of this argument is that different network structures evolve depending on the prioritization of aims. For example, economic goals may push networks toward adopting relatively efficient core-and-periphery structures that more closely resemble hierarchical businesses while sheltering the most central elements, whereas political goals might create incentives for cell structures that maximize security so that long-term goals can be pursued.

Small Arms Trafficking

Some illicit arms trafficking networks have long-term political goals, especially those connected to diasporas supporting armed groups operating in their homelands. However, most participants on the supply side of the illicit arms trade are out to turn a profit in a competitive black market. Consequently, small arms trafficking networks are more likely to be structured in ways that compromise their security, all else being equal. Some suppliers, brokers, or transporters may operate in market niches, most likely attached to particular geographic locales, and therefore face little competition, but others must devote some of their energies to outmaneuvering others for clients. They also increase their take by squeezing those they must deal with up and down the supply and distribution chain. Such imperatives are not different in kind from the competitive forces operating in legal markets, but the temptation to defect and “rat out each other” is undoubtedly present and may ultimately threaten to undermine the mutual trust and reciprocity that seem essential for the functioning of illicit networks. How this tension is resolved is likely to depend on the structural characteristics of particular networks and the attributes of those who participate in the enterprise.

Competitive dynamics within these networks, along with a generally high volume of small arms trafficking activity, work against concealment and create vulnerabilities. Bruinsma and Bernasco (2004) have examined three criminal groups whose activities have two important features in common with illicit small arms trafficking other than the need to operate underground. Heroin smuggling, human trafficking, and the transnational trade in stolen cars serve a market and involve the movement of illegal goods and services across long distances. Bruinsma and Bernasco find that activities characterized by higher levels of criminal and financial risk require collaboration grounded on substantial mutual trust, which is typically a feature of criminal enterprises that have cohesive social network structures underpinning them. In the case of heroin smuggling, the riskiest of the three criminal enterprises examined, that cohesion derives from ethnic and other demographic homogeneities. Turkish groups figure prominently in the heroin trade (at least destined for the Netherlands, a focus of the Bruinsma and Bernasco study); those who work most closely together at the different stages of the process tend to be of similar age and social class and hail from the same regions of the country.

It is difficult to say whether, in terms of criminal and financial risk, the illicit small arms trade has more in common with heroin smuggling or purportedly less-risky trafficking in humans or stolen automobiles. But a reasonable hypothesis is that illicit arms networks that operate in higher risk environments—for example, in geographic locales with a robust police and/or military presence, or spanning long distances with multiple sites of potential vulnerability—must be grounded in dense social network structures to be effective and resilient. The social cohesion created by ethnic, religious, or ideological bonds reduces the likelihood of defection and thus the risks of exposure in an extralegal setting.

In addition to dense social ties that give rise to cohesion, temporary “shortcuts” can be created in these networks to facilitate information transfer and more effective coordination within the network (e.g., Krebs, 2002). Yet even in regard to security, as Montgomery (2005, 170) points out, decentralized but densely connected networks have their own vulnerabilities:

> Densely connected, decentralized networks where no single node holds a crucial position in the network are easier in one sense to shut down: connections to additional nodes in the network are easier to discover, although this is balanced by the number of nodes and connections that need to be eliminated to dissolve the network.

Weapons of Mass Destruction Trafficking

Ballistic missile and WMD proliferation networks form around longer-term and considerably more challenging goals than do small arms trafficking networks. When proliferation networks serve the interests of states, the goal is to significantly enhance the military capability (and prestige) of the state by providing resources and know-how necessary to develop weaponry that relatively few other states possess (Kroenig, 2010). The scarcity of supply (components, machinery, knowledge, etc.) and the stringency of regulations intended to prevent proliferation require patience and perseverance over longer periods of time.

Historically, the transfer of expertise, materials, technology, or assembled weapons has been viewed as more immoral than illegal; “sensitive” assistance has long been a staple of nuclear weapons proliferation, even if the tacit knowledge requirements have limited the effectiveness of these transfers, structuring the nuclear proliferation network as a set of hubs rather than the denser and more reciprocal missile proliferation network (Montgomery 2005, 2008, 2013); see figure 1.

Click to view larger

Figure 1: Nuclear (top, data from Kroenig, 2010) and ballistic missile (bottom, data from Montgomery, 2008) proliferation networks.

The demand for WMD and effective delivery vehicles varies by type of weapon and by the particular motivations of the potential recipients. While nuclear, chemical, and biological weapons have generally been complements when states are engaged in the pursuit of such capabilities (Horowitz and Narang, 2014), countries that actually succeed in acquiring nuclear weapons have generally been willing to give up pursuit of the others. Militant organizations generally seek WMD if they are embedded in alliance structures and based in authoritarian countries with relatively strong connections to a globalized world; however, contrary to popular expectations, there is little evidence that suggests a correlation with religious ideology (Asal, Ackerman, and Rethemeyer, 2012).

When proliferation networks operate on behalf of nonstate actors—for example, attempting to acquire radioactive material for a dirty bomb[3] or chemical precursors for sarin—the goal is to enhance the group's ability to attack and terrorize its enemies rather than to provide the group with a sustainable WMD or ballistic missile capability. Nevertheless, the sort of groups seeking the ability to launch such spectacular attacks are also likely to be motivated by longer-term political goals, which suggests that, like the proliferation networks serving states, these networks are also likely to prioritize security over efficiency in meeting their objectives.

Countering Illicit Networks

Network forms of organization seem to offer distinct advantages to those engaged in illicit economic, political, and military activities. As Kenney (2007, 203) explains, compared to the hierarchically organized and bureaucratic state agencies—intelligence, law enforcement, or military—that typically oppose them, illicit networks

> contain relatively flat authority structures that facilitate rapid decision cycles and quick information flows. They compartment participants and information into separate, semiautonomous cells, often based on family, friendship, and geographic ties. They build redundancy into their operations by giving important functions to multiple groups, and they rely on brokers and other intermediaries to span "structural holes" between loosely connected nodes and networks.

These organizational structures and practices foster secrecy and secure the distribution of information and other resources necessary to accomplish tasks. State agencies enjoy a preponderance of coercive force and intelligence collection capacity. Yet their ability to employ these capacities to penetrate illicit networks and track their activities can be constrained by elaborate decision-making procedures, organizational checks, and other imperatives. And when state agencies are successful—for example, when they capture or kill a drug kingpin or terrorist mastermind and consequently are able to dismantle a portion of the illicit enterprise—this often proves temporary, as others regroup, reorganize, and recruit new members into more diffuse network structures (Johnston, 2012; Jordan, 2009, 2014). Thus, adopting network structures provides organizational advantages that can be deployed against adversaries with superior resources but operating within the constraints of bureaucratic and hierarchical organizations (Williams, 2001).

Yet these network structures can have major disadvantages in terms of command and control, information transmission, replication of roles, and even robustness against attack if critical bridging nodes are eliminated or structures are decentralized but still dense. Moreover, states can and do respond to network structures by adapting their own methods accordingly; the response to WMD proliferation networks, for example, has included a semi-institutionalized, informal set of norms and principles under the Proliferation Security Initiative (Caves, 2006). However, the overall effectiveness of PSI as a networked entity as opposed to a formal organization or simple bilateral efforts is unclear (Valencia, 2007), and formalized ties are quite useful for counterproliferation, especially in the financial arena (Schlumberger and Gruselle, 2007).

Centrality and Centralization in Weapons Networks

In addition to the overall advantages and disadvantages of adopting network forms of organization to strike different balances of efficiency and security, social scientists are interested in actors' relative power within them, the overall degree of centralization of the network as a whole, and the multiple overlapping layers that constitute most networks. Actors occupying particular central positions have access to resources that can be exploited to pursue individual and collective interests (Hafner-Burton, Kahler, and

Montgomery, 2009; Kahler, 2009). The resources available to suppliers, middlemen, shippers, and others involved in the transfer of illicit weaponry are both material and social. Those who possess or can muster superior armament stocks, finance, transport, and other material resources are in a better position to exercise power within the network than those who do not. But one's access is also a key source of influence and success. Compared to legal arms markets, where openly publicizing the availability of goods and distribution services is not a risky enterprise, the contribution of social connections to one's ability to survive and thrive in the illicit market takes on relatively greater importance. Larger numbers of relationships provide more opportunities for profitable transaction, but so do the right types of relationships. The pivotal activities of arms brokers, who bring together parties that would not otherwise come into contact in an underground environment, epitomize the role that social capital plays in illicit weapons networks (Amnesty International, 2006; Cattaneo, 2004; Peleman and Wood, 2000).

Distinctive network structures arise from the frequency and intensity of interaction among network actors, whether they be individuals or collective entities. Those structures suggest certain things about the efficiency with which goods and information move from one part of the network to another, as well as the vulnerability of these flows to disruption. Second-tier nuclear proliferation networks—those that connect actors in post-1967 proliferant states and serve those states' nuclear ambitions—tend to be rather centralized, with a few highly connected nodes positioned as hubs and a larger number of nodes with links to the central nodes but few direct connections among themselves (Braun and Chyba, 2004; Gruselle, 2007; Montgomery, 2005, 2008). The A. Q. Khan network, fully exposed in 2004, displayed this sort of star structure. The network's hub was, of course, Khan himself (and Khan Research Laboratories), in Pakistan, with links to other nodes in Iran, North Korea, Libya, and elsewhere.

Ballistic missile technology has also proliferated through second-tier networks exhibiting star structures, with North Korea and Iran as hubs, although these tend to be less centralized than nuclear proliferation networks (see figure 1). Even "first-tier" nuclear assistance has often appeared to be centralized, with each nuclear program attempting to take advantage of prior or concurrent nuclear programs through spying (Reed and Stillman, 2009), although it is still debated how useful most of this assistance has been (Kroenig, 2010; Montgomery, 2013). The A. Q. Khan network demonstrates both the advantages and disadvantages of network structures for proliferation: while it enabled first Pakistan and then Iran, Libya, and North Korea to take advantage of Khan's diffuse supply network, it also generated a wealth of indicators and warnings for intelligence communities to map the network before rolling it up (Albright, Brannan, and Stricker, 2010; Corera, 2006; Montgomery, 2005, 2013). Similarly, Aum Shinrikyo's acquisitions

could have provided early indicators of its intentions before the Tokyo subway sarin gas attacks (Picarelli, 1998).

One reason for the greater centralization of WMD proliferation networks and their tendency to manifest star structures is the importance of tacit knowledge in the development of nuclear and (to a lesser extent) ballistic missile capability (Montgomery, 2005, 2008). The components and precision machinery needed to produce nuclear bombs and rocketry are difficult to acquire, but the knowledge and experience necessary to take the intermediate steps from weapon designs to functioning finished systems may present the bigger hurdle. Yet even these two types of networks differ significantly; there are many small, tacit knowledge problems with missile technologies that allow for collaboration, whereas for nuclear weapons the engineering issues provide significant barriers to knowledge transmission. There are even fewer holders and willing purveyors of tacit knowledge than there are of the other elements that must be brought together to succeed at this level of weapons development, and they are likely to be coterminous with the few hubs in proliferation networks. However, proliferants can also take the “street-legal” proliferation route by seeking to acquire capabilities through the transfer of civilian nuclear technologies, which can sometimes be an indicator of nuclear weapons intentions (Fuhrmann, 2012; Morstein and Perry, 2000).

Thus, the centralized nature of nuclear and ballistic missile proliferation networks reflects the advanced knowledge required for the development of this type of weaponry, scarcity of components and manufacturing technology, and the long-standing regulatory efforts of states. None of these apply to SALW: they are not difficult to manufacture, there is abundant surplus, and distribution is not closely regulated (the 2014 Arms Trade Treaty notwithstanding). So it is not surprising that illicit networks operating in this realm tend to exhibit more decentralized structures. The number of participants in these networks is far greater, and they are located in far more states. Although the individuals and groups involved in the illicit small arms trade do not always have many connections to other actors, some do. These networks are more diffuse than WMD proliferation networks and more closely resemble clique structures, in which nodes are connected to each other directly rather than indirectly through hubs. That is not always the case, however, and when the state is the level of analysis, some state locales are substantially more active as origination points and destinations of illicit weaponry, as well as transshipment points. States in the former Soviet bloc, for example, stand out as more central nodes in the illicit flow of arms to African conflict zones and thus form geographic hubs in an otherwise dense global network (Kinsella, 2006, 2014).

Multiplex Network Structures and Geography

Proliferation and small arms networks are not simply social or political networks; they also are—or are conjoined with—physical networks. These networks also contain multiple layers: the layer representing direct assistance between states looks very different from the layers involving, for example, middlemen who procure components, transporters who facilitate the movement of the components themselves (Hastings, 2012), and brokers who arrange financing (Group d'action financiere, 2008; Gruselle, 2007). Each country's internal and external proliferation network differs depending on political structures, international barriers, and other factors like active diasporas (Boureston and Russell, 2009). Existing smuggling networks for other goods can also be reused for the acquisition and transfer of unconventional weaponry, by both states and nonstate actors (see, e.g., Chestnut [2007] on North Korea and Frost [2014] on Latin America).

Because proliferation and small arms networks move contraband from one location to another, the physical and political geography of that space may help to explain the behavior of illicit actors and the structure of their networks. For example, several factors have conspired to make individuals and organizations in Russia and other former Soviet bloc locales active participants in illicit arms transfer networks. The most common explanations focus on the role of military and security forces, especially the incentives and opportunities associated with the political-economic transition that accompanied the end of the Cold War (Gerasev and Surikov, 1997; Holloway and McFaul, 1995; Turbiville, 1996). In addition to arms surpluses, they had access to military transport facilities or found common cause with others who had logistical expertise and experience moving cargo surreptitiously. Well-developed transportation infrastructures plus the uncertainties of postcommunism (features of multiple state locales clustered geographically in Eastern Europe and Central Asia) help to account for their emergence as pivotal nodes in illicit arms supply networks.

In regard to proliferation networks, Hastings (2012, 431) proposes a geographic approach that focuses 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." The structure and geographic layout of these networks depend on the extent to which the state is actively engaged in the illicit deal making, financial transactions, and physical movement of goods. In some cases, those coordinating the transfer of nuclear material, machinery, and other necessary components have access to resources of sovereign states, namely transportation infrastructure, controlled borders, and diplomatic prerogative. Weapons of mass destruction proliferation networks generally involve states, and therefore those engaged in illicit activities on their behalf

have access to state resources. While working on behalf of his home government beginning in the 1970s, A. Q. Khan's network had access to Pakistan's diplomatic outposts and military transport, and once foreign-sourced materiel arrived on Pakistani territory or at its ports, there was little need to worry that state authorities would prevent it from arriving at prescribed destinations.

Non-state-based WMD proliferation networks are more like free agents and have little or no access to state resources. In conducting their illicit transactions and transfers, they are compelled to seek out the most hospitable environments available without the benefit of state sponsorship or prerogatives. These networks must therefore make use of the commercial transportation infrastructure, and in doing so they gravitate to geographic locales where their activities will be most secure from exposure and disruption. Those are the places where network hubs form. Hastings (2012) thus observes that when A. Q. Khan (as a semi-independent agent)[4] redirected his efforts to Libya's nuclear ambitions in the 1990s, he could no longer count on the resources of his home state. The network's primary hub formed in the United Arab Emirates, which attracts a large number of foreigners (and foreign companies) and whose geographic location and advanced port facilities accommodate a great deal of global commerce.

The implications for the structure of WMD proliferation networks are twofold. First, networks without access to state resources are more likely to develop global reach in order to seek out weapons components that are scarce, because of their sophistication, but nonetheless available because political and economic conditions (and sometimes personal connections) permit illicit transfer. This is not a strength; it is required to maximize network security when state resources are unavailable to the network. And it comes at the expense of efficiency. Second, although these networks may be spread thin globally, illicit transactions are concentrated at nodes that are, of necessity, established to take advantage of commercial infrastructure. In this respect, the networks are more centralized than state-sponsored, second-tier WMD proliferation networks, which are territorially diffuse because their logistics can take advantage of a multitude of diplomatic outposts and a state-controlled transportation infrastructure. Although the latter appear to have star structures when nodes are operationalized as state locales, they are likely to manifest considerably less centralized structures when nodes represent network actors operating in more precisely specified geographic locations.

The geography of ballistic missile proliferation networks, and perhaps even illicit small arms networks, ought to exhibit the same patterns that Hastings (2012) observes in the case of nuclear proliferation networks. However, compared to nuclear and ballistic missile proliferation, a much smaller proportion of total illicit small arms trafficking activity is sponsored by states. This is because states have far less need to turn to illicit networks when they want to acquire this type of weaponry, which is generally (but not

always) a legitimate activity for states and easy to accomplish given the large number of suppliers. When states do engage in illicit small arms networks, this is usually in the role of covert suppliers of weapons destined for insurgencies and/or contravening multilateral arms embargoes. It follows, then, that illicit arms networks that connect to state suppliers, because they have access to state-controlled assets and infrastructure, will be territorially diffuse and less centralized. Where states are not involved, and state resources are unavailable to arms traffickers, the geography of illicit small arms networks may more closely align with the nodes and routes constituting the commercial transportation infrastructure. Thus, they should exhibit more centralized structures.

Arms Data and Network Analysis

Implicit in our discussion of arms trafficking and proliferation networks is the notion that these are purposeful organizations engaged in collective action. That is, these networks are collective actors whose organizational forms have evolved in ways more or less conducive to the transfer of weapons, nuclear material, processing equipment, and so forth, in a covert and insecure environment. Not all participants in these networks have their eyes on the prize—the arrival of illicit weapons or components at the intended destination—and many are motivated solely by opportunism and the individual gains they derive from whatever role they play in the process. But in the aggregate, these networks resemble purposeful organizational entities, and arrayed against them are other purposeful actors like law enforcement or other state agencies charged with disrupting them.

Empirical investigation into the activities and structure of A. Q. Khan’s proliferation network or the arms-transport network assembled by Viktor Bout and associates, not to mention other “dark networks” like Cosa Nostra or al-Qaeda, generally takes for granted that these entities take the form of networked organizations. Social network analysis can then be applied to discover the structural features of these networks, key players within them, organizational strengths and vulnerabilities, and so forth. The outer bounds of these organizations may or may not be clearly discernible—who is part of the network, who is not—but these networks can reasonably be conceptualized as actors.

However, the application of network concepts and analytical methods need not presume that a particular collection of nodes constitutes a purposeful organization in the sense that we have been discussing illicit arms and proliferation networks in this chapter. Indeed, SNA in the field of international relations frequently examines the structure of interstate relations, such as conflict or trade, in an effort to gain empirical insights that may be missed by other methodologies, but without any presumption that states are

organized (networked) for collective action (e.g., Hafner-Burton, Kahler, and Montgomery, 2009; Maoz, 2011). They may be, as would be true of states in a military alliance or a free trade association, but international interactions more generally can exhibit network-like patterns. Here “network” describes a structure of interaction without implying collective action per se.

These observations concerning networks as actors versus networks as structures are particularly relevant to arms trade research, as we describe below. Illicit small arms transfers, for example, are commonly facilitated by trafficking networks (actors), while global arms flows, both legal and illegal, exhibit patterns commonly associated with networked organizational forms (structures). To date, there have been few network analytic studies at either level of analysis.

Data Sources and Studies

Quantitative network analysis requires, at a minimum, data identifying nodes and the presence or absence of links between them. Ideally, in the case of proliferation and arms networks, we would like to have information on the individuals (dealers, brokers, financiers, etc.) and collective entities (manufacturers, transport companies, government agencies, insurgencies, etc.) involved in the transfers, as well as type and volume of what is exchanged (weapons, enrichment machinery, cash, etc.). We would also like to have data on the locations of these actors and their transactions, given the geographic factors that influence the behavior and structure of these networks. Needless to say, systematic and reliable information at this level of detail is not readily available for illicit networks like those we have been discussing. Where systematic and reasonably comprehensive data do exist, they are likely to be aggregated by state, even when states (or their agents) are not network actors per se, but merely the geographic locales within which actors operate. Finer-grained information, which is often the result of law enforcement activities or investigative journalism, is available for many networks, but these data are not very comprehensive and are difficult to assemble in a systematic way.

The most authoritative source of both quantitative and qualitative information on the arms trade is the yearbook published by SIPRI, *Armaments, Disarmament and International Security*.[5] SIPRI relies exclusively on open sources for its data and focuses its attention on the kind of information consistently available to the public, namely MCW systems. These include aircraft, armor and artillery, guidance and radar systems, missiles, and ships. In addition to those items physically transferred to recipients, SIPRI includes weaponry manufactured by the recipient under license. The MCW data come in two forms: “trade registers” of transferred military hardware broken down by model (F-16 aircraft, M-60 tanks, Patriot surface-to-air missile systems, etc.) and dollar-valued

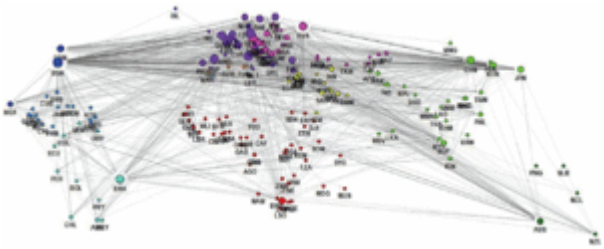
aggregates. The latter do not represent what the recipient paid for arms; they represent the “military resource value” of transferred weaponry based on performance characteristics.[6]

The few studies that take a network approach to the MCW trade all make use of the SIPRI data. Some deploy SNA for primarily descriptive purposes, especially for visualization (e.g., Kinsella, 2003), even if they go on to model dyadic relations using standard econometric methods (e.g., Akerman and Seim, 2014). That is, the importance of network-level processes in arms trading is acknowledged in these studies, but not actually incorporated into inferential models for purposes of hypothesis testing. Two recent exceptions are Willardson (2013) and Thurner et al. (2015). Both studies make use of exponential random graph models (ERGMs) to identify the covariates of arms trading while factoring in structural features of the global arms market. In terms of our discussion above, such studies treat networks not as actors, but as structures. We expect that the SIPRI data will continue to be examined using these and increasingly sophisticated network analytic methods, bringing new insights to what we already know (or think we know) from the extensive quantitative literature on the global arms trade (see Kinsella, 2011).

As the attention of the academic and policy communities has turned increasingly to SALW, there has been a great deal of interest in the collection and distribution of systematic information (qualitative and quantitative) on this aspect of the arms trade. Because the SALW trade is much less regulated by state authorities than the major weapons trade, and because the weapons themselves are smaller and harder to observe by journalists and others who might want to document their movement, reliable information is very difficult to gather on a consistent basis. But researchers are now beginning to accumulate and release pertinent data.[7] Most promising for network analysis are the data collected by the Norwegian Initiative on Small Arms Transfers (NISAT), located at the International Peace Research Institute in Oslo. In addition to its document library, NISAT maintains an online database of SALW transfers, with some records dating back to 1962. These data are likely to feature in future academic and policy research and are well suited to network analysis and visualization.[8]

As an illustration, figure 2 maps the global trade in SALW based on NISAT data for 1998–2005. The nodes are states, which are labeled with three-letter country codes, arranged according to the geographic coordinates of their capital cities, and color-coded by region. A line connecting any two nodes means that SALW transfers between them totaled more than $1 million during the period, with thicker and darker lines indicating higher transfer volumes. The size of the nodes corresponds to the state’s centrality in the network, operationalized here as outdegree: the number of other states that were recipients of that

state's SALW exports. The most central nodes in this network are the United States, several states in Western Europe, Russia, and Brazil.



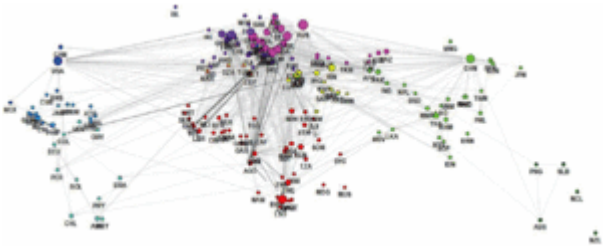
Click to view larger

Figure 2. Legal small arms trade: node size as outdegree centrality

The value of the SALW trade amounts to roughly $4 billion per year, and probably 10 to 20 percent of this occurs in the black and gray markets. In addition to collecting quantitative data on the legal SALW trade, NISAT maintains the Black Market File Archive, a collection of news stories and investigative reports on the illicit arms trade. This material can be coded for use in network analysis (see Kinsella, 2008), although the stories and reports collected by NISAT vary widely in the amount of useful information they contain. Some articles include detailed accounts of arms shipments from manufacturer to purchaser, including any number of participating intermediate dealers, brokers, and shipping agents. Other reports include no codable event information at all. Some reports provide a wealth of background information, such as previous events in ongoing arms-supply relationships. Others pick up a particular shipment's journey midstream, such as when one militant group supplies another, without any indication of where the first group acquired the weaponry. Even when reports contain complete information, the events themselves exhibit a wide range of forms. There is substantial variation in the number and type of intermediaries engaged in illicit transfers, the nature of the illegalities involved (forged end-user certificates, arsenal theft, etc.), and whether transfers were intercepted by state authorities or someone other than the intended recipient.

Despite these limitations, this information can be used to generate binary network data, which can then be examined to elucidate the contours of illicit arms trading at regional and global levels (e.g., Kinsella, 2006, 2014). For example, following the format of figure 2, figure 3 uses these data to map illicit arms transfers between states. Here the lines connecting the nodes indicate that illicit weapons flowed from one state to the other at least once during the 1998–2005 period. Although governments are sometimes complicit in these transfers, usually they are not, so the nodes in this network are state locales: geographic spaces within which participants in the illicit arms trade operate. The lines connecting the nodes are thicker and darker if there are more illicit arms-transfer events ascertained from the reports in the NISAT archives; they do not indicate the volume of the arms flow, either in quantity or value, which is not sufficiently documented. The

prominence of former Soviet-bloc countries in the illicit arms trade is noteworthy. The three locales with the highest outdegree centralities are Russia, Czech Republic, and Bulgaria, while the former Soviet bloc constitutes half of the twenty most central nodes worldwide.



Click to view larger

Figure 3. Illicit arms trade: node size as outdegree centrality

Figure 3 further highlights the links between and among the former Soviet-bloc countries and locales in sub-Saharan Africa, which constitute over one-third of the 650 links shown in figure 2. Of these, over 40 percent represent outflow links from the former Soviet bloc to sub-Saharan Africa, while just under 40 percent are links within sub-Saharan Africa. Figure 4 also shows the substantial number of links among former Soviet-bloc locales.

Click to view larger

Figure 4. Illicit arms trade: former Soviet bloc and sub-Saharan Africa

As in figure 2, analysis of data displayed in figures 3 and 4 proceeds from a conceptualization of networks as structures rather than purposeful actors. There are exceedingly few social network analyses of illicit arms trafficking networks, in contrast to other criminal organizations, despite an otherwise fairly developed scholarly and policy-oriented literature on such groups, many of which I have cited in this chapter. Curwen's (2007) study of the illicit network of suppliers, brokers, financiers, and transportation agents involved in the transfer of weapons to Liberia between 1999 and 2002 is one example, although his analysis is limited to the use of network visualizations and the computation

of descriptive statistics like centrality. Attempts to broaden this type of network-as-actor analysis over space and time will confront substantial data collection hurdles. However, much raw material exists in NISAT's Black Market File Archive, and text-mining algorithms designed for the extraction of network data could prove useful for systematizing it (e.g., Carley, Columbus, and Landwehr, 2013).

Finally, due to the small number of cases, WMD transfers are also primarily analyzed graphically rather than quantitatively as a network. Data sets on both sensitive (Kroenig, 2010) and civilian (Fuhrmann, 2012) nuclear transfers exist, and missile transfers (Montgomery, 2008) can be gleaned from Nuclear Threat Initiative country reports. However, little or no information has been systematically collected on chemical and biological weapons transfers, although intentional incidents of both fortunately appear to be relatively infrequent.

Conclusion

The study of the transfer of SALW, MCW, and WMD is ripe for the use of network theories and methods. Yet so far there has been little quantitative or qualitative network analysis of these networks. Rather, most work has consisted of hypotheses regarding the advantages and disadvantages of particular types of network structures for these transfers. This is partially due to a lack of reliable data sets, which is in turn due in part to the illicit and clandestine nature of most of these relationships and transactions. We have focused most of our discussion on SALW and WMD rather than on MCW because of the more extensive literature on the former two with respect to network structures. Yet the lack of analysis of the latter as a network (rather than as a set of dyads in a traditional gravity model) is somewhat puzzling given the greater availability of data and the lack of additional confounding factors.

We clearly do not lack for hypotheses regarding network structures in this area of research, just analysis. Consequently, this area is clearly ripe for the application of network theories to extant data sets using network methods and for the collection of new data for network analysis. Given the general import of these networks for both security studies and policy relevance, we expect to see a renaissance in the study of arms supply and proliferation networks.

References

Akerman, A., and Seim, A. L. (2014). "The Global Arms Trade Network 1950–2007." *Journal of Comparative Economics* 42(3): 535–551. doi:10.1016/j.jce.2014.03.001.

Albright, D., Brannan, P., and Stricker, A. S. (2010). “Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan.” *Washington Quarterly* 33(2): 85–106. doi: 10.1080/01636601003673857.

Amnesty International. (2006). “Dead on Time—Arms Transportation, Brokering and the Threat to Human Rights.” .

Asal, V. H., Ackerman, G. A., and Rethemeyer, R. K. (2012). “Connections Can Be Toxic: Terrorist Organizational Factors and the Pursuit of CBRN Weapons.” *Studies in Conflict & Terrorism* 35(3): 229–254. doi:10.1080/1057610X.2012.648156.

Bakker, R. M., Raab, J., and Milward, H. B. (2012). “A Preliminary Theory of Dark Network Resilience.” *Journal of Policy Analysis and Management* 31(1): 33–62.

Boureston, J., and Russell, J. A. (2009). “Illicit Nuclear Procurement Networks and Nuclear Proliferation: Challenges for Intelligence, Detection, and Interdiction.” *St. Antony’s International Review* 4(2): 24–50.

Braun, C., and Chyba, C. F. (2004). “Proliferation Rings: New Challenges to the Nuclear Nonproliferation Regime.” *International Security* 29(2): 5–49.

Bruinsma, G., and Bernasco, W. (2004). “Criminal Groups and Transnational Illegal Markets.” *Crime, Law and Social Change* 41(1): 79–94. doi:10.1023/B:CRIS. 0000015283.13923.aa.

Buzan, B., and Herring, E. (1998). *The Arms Dynamic in World Politics*. Boulder, CO: Lynne Rienner Publishers.

Carley, K. M., Columbus, D., and Landwehr, P. (2013). “AutoMap User’s Guide 2013.” CASOS Technical Report CMU-ISR-13-105. Center of the Computational Analysis of Social and Organization Systems, Carnegie Mellon University. .

Cattaneo, Silvia. (2004). “Targeting the Middlemen: Controlling Brokering Activities.” In *Small Arms Survey 2004: Rights at Risk*, edited by P. Batchelor and K. Krause, pp. 140–171. Oxford: Oxford University Press.

Caves, J. P., Jr. (2006). “Globalization and WMD Proliferation Networks: The Policy Landscape.” *Strategic Insights* 5(6): .

Chestnut, S. (2007). “Illicit Activity and Proliferation: North Korean Smuggling Networks.” *International Security* 32(1): 80–111. doi:10.1162/isec.2007.32.1.80.

Corera, G. (2006). *Shopping for Bombs: Nuclear Proliferation, Global Insecurity, and the Rise and Fall of the A.Q. Khan Network*. Oxford: Oxford University Press.

Curwen, P. A. (2007). “The Social Networks of Small Arms Proliferation: Mapping an Aviation Enabled Supply Chain.” Master’s thesis, Naval Postgraduate School.

Enders, W., and Su, X. (2007). “Rational Terrorists and Optimal Network Structure.” *Journal of Conflict Resolution* 51(1): 33–57. doi:10.1177/0022002706296155.

Eyre, D. P., and Suchman, M. C. (1996). “Status, Norms, and the Proliferation of Conventional Weapons.” In *The Culture of National Security: Norms and Identity in World Politics*, edited by P. J. Katzenstein, pp. 186–215. New York: Columbia University Press.

Frost, J. R. (2014). “The Nexus Between Criminal and Extremist Groups in Latin America: Implications for Unconventional Weapons Acquisition.” PhD thesis, George Mason University. .

Fuhrmann, M. (2012). *Atomic Assistance: How “Atoms for Peace” Programs Cause Nuclear Insecurity*. Ithaca, NY: Cornell University Press. .

Gerasev, M., and Surikov, V. M. (1997). “The Crisis in the Russian Defense Industry: Implications for Arms Exports.” In *Russia in the World Arms Trade*, edited by A. J. Pierre and D. Trenin, pp. 9–25. Washington, DC: Carnegie Endowment for International Peace.

Grimmett, R. F., and Kerr, P. K. (2012). “Conventional Arms Transfers to Developing Nations, 2004-2011.” CRS Report R42678.

Group d’action financiere. (2008). “Proliferation Financing Report.” Financial Action Task Force. .

Gruselle, B. (2007). “Proliferation Networks and Financing.” Foundation pour la Recherche Strategique. .

Hafner-Burton, E. M., Kahler, M., and Montgomery, A. H. (2009). “Network Analysis for International Relations.” *International Organization* 63(3): 559–592. doi:10.1017/S0020818309090195.

Hämmerli, A., Gattiker, R., and Weyermann, R. (2006). “Conflict and Cooperation in an Actors’ Network of Chechnya Based on Event Data.” *Journal of Conflict Resolution* 50(2): 159–175. doi:10.1177/0022002705284826.

Hastings, J. V. (2012). “The Geography of Nuclear Proliferation Networks.” *Nonproliferation Review* 19(3): 429–450. doi:10.1080/10736700.2012.734190.

Holloway, D., and McFaul, M. (1995). “Demilitarization and Defense Conversion.” In *The New Russia: Troubled Transformation*, edited by G. W. Lapidus, pp. 193–222. Boulder, CO: Westview Press.

Holtom, P. (2009). “Reporting Transfers of Small Arms and Light Weapons to the United Nations Register of Conventional Arms, 2007.” SIPRI Background Paper. .

Horowitz, M. C., and Narang, N. (2014). “Poor Man’s Atomic Bomb? Exploring the Relationship between ‘Weapons of Mass Destruction.’” *Journal of Conflict Resolution* 58(3): 509–535. doi:10.1177/0022002713509049.

Johnston, P. B. (2012). “Does Decapitation Work? Assessing the Effectiveness of Leadership Targeting in Counterinsurgency Campaigns.” *International Security* 36(4): 47–79. doi:10.1162/ISEC_a_00076.

Jordan, J. (2009). “When Heads Roll: Assessing the Effectiveness of Leadership Decapitation.” *Security Studies* 18(4): 719–755. doi:10.1080/09636410903369068.

Jordan, J. (2014). “Attacking the Leader, Missing the Mark.” *International Security* 38(4): 7–38. doi:10.1162/ISEC_a_00157.

Kahler, M. (Ed.). (2009). *Networked Politics: Agency, Power, and Governance*. Ithaca, NY: Cornell University Press. .

Kenney, M. (2007). *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation*. University Park: Pennsylvania State University Press. .

Kinne, B. J. (2014). “Dependent Diplomacy: Signaling, Strategy, and Prestige in the Diplomatic Network.” *International Studies Quarterly* 58(2): 247–259. doi:10.1111/isqu.12047.

Kinsella, D. (2003). “Changing Structure of the Arms Trade: A Social Network Analysis.” Presented at the Annual Meeting of the American Political Science Association, Philadelphia, PA. .

Kinsella, D. (2006). “The Black Market in Small Arms: Examining a Social Network.” *Contemporary Security Policy* 27(1): 100–117. doi:10.1080/13523260600603105.

Kinsella, D. (2008). “Illicit Arms Transfers Dataset: Coding Manual.” Portland State University. .

Kinsella, D. (2011). “The Arms Trade.” In *The Handbook on the Political Economy of War*, edited by C. J. Coyne and R. L. Mathers, pp. 217–242. Northampton, MA: Edward Elgar Publishing.

Kinsella, D. (2014). “Illicit Arms Transfers to Africa and the Prominence of the Former Soviet Bloc: A Social Network Analysis.” *Crime, Law and Social Change* (August): 1–25. doi:10.1007/s10611-014-9531-9.

Kinsella, D., and Chima, J. S. (2001). “Symbols of Statehood: Military Industrialization and Public Discourse in India.” *Review of International Studies* 27(3): 353–373. doi: 10.1017/S0260210501003539.

Kleemans, E. R., and Van De Bunt, H. G. (1999). “Social Embeddedness of Organized Crime.” *Transnational Organized Crime* 5(1): 19–36.

Klerks, P. (2001). “The Network Paradigm Applied to Criminal Organizations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands.” *Connections* 24(3): 53–65.

Koschade, S. (2006). “A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence.” *Studies in Conflict and Terrorism* 29(6): 589–605. doi:10.1080/10576100600798418.

Krebs, V. E. (2002). “Mapping Networks of Terrorist Cells.” *Connections* 24(3): 43–52.

Kroenig, M. (2010). *Exporting the Bomb: Technology Transfer and the Spread of Nuclear Weapons*. Ithaca, NY: Cornell University Press.

Lampe, K. v., and Johansen, P. O. (2004). “Organized Crime and Trust:: On the Conceptualization and Empirical Relevance of Trust in the Context of Criminal Networks.” *Global Crime* 6(2): 159–184. doi:10.1080/17440570500096734.

Lindelauf, R., Borm, P., and Hamers, H. (2009). “The Influence of Secrecy on the Communication Structure of Covert Networks.” *Social Networks* 31(2): 126–137. doi: 10.1016/j.socnet.2008.12.003.

Mac Ginty, R. (2010). “Social Network Analysis and Counterinsurgency: A Counterproductive Strategy?” *Critical Studies on Terrorism* 3(2): 209–226. doi: 10.1080/17539153.2010.491319.

Maoz, Z. (2011). *Networks of Nations: The Evolution, Structure, and Impact of International Networks, 1816–2001*. Structural Analysis in the Social Sciences 32. Cambridge, UK: Cambridge University Press.

Milward, H. B., and Raab, J. (2006). “Dark Networks as Organizational Problems: Elements of a Theory.” *International Public Management Journal* 9(3): 333–360. doi: 10.1080/10967490600899747.

Montgomery, A. H. (2005). “Ringing in Proliferation: How to Dismantle an Atomic Bomb Network.” *International Security* 30(2): 153–187.

Montgomery, A. H. (2008). “Proliferation Networks in Theory and Practice.” In *Globalization and WMD Proliferation: Terrorism, Transnational Networks, and International Security*, edited by J. A. Russell and J. J. Wirtz, pp. 28–39. .

Montgomery, A. H. (2013). “Stop Helping Me: When Nuclear Assistance Impedes Nuclear Programs.” In *The Nuclear Renaissance and International Security*, edited by A. Stulberg and M. Fuhrmann, pp. 177–202. Stanford, CA: Stanford University Press.

Morselli, C., Giguère, C., and Petit, K. (2007). “The Efficiency/Security Trade-off in Criminal Networks.” *Social Networks* 29(1): 143–153. doi:10.1016/j.socnet.2006.05.001.

Morstein, J. H., and Perry, W. D. (2000). “Commercial Nuclear Trading Networks as Indicators of Nuclear Weapons Intentions.” *Nonproliferation Review* 7(3): 75–91.

Murji, K. (2007). “Hierarchies, Markets and Networks: Ethnicity/Race and Drug Distribution.” *Journal of Drug Issues* 37(4): 781–804. doi:10.1177/002204260703700403.

Naylor, R. T. (2004). *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Ithaca, NY: Cornell University Press.

Parkinson, S. E. (2013). “Organizing Rebellion: Rethinking High-Risk Mobilization and Social Networks in War.” *American Political Science Review* 107(3): 418–432. doi: 10.1017/S0003055413000208.

Peleman, J., and Wood, B. (2000). “The Arms Fixers. Controlling the Brokers and Shipping Agents.” Joint Report of BASIC, NISAT, and PRIO. .

Perliger, A., and Pedahzur, A. (2011). “Social Network Analysis in the Study of Terrorism and Political Violence.” *PS: Political Science & Politics* 44(01): 45–50. doi:10.1017/S1049096510001848.

Picarelli, J. T. (1998). “Transnational Threat Indications and Warning: The Utility of Network Analysis.” AAAI Fall Symposium on Artificial Intelligence and Link Analysis. .

Pokalova, E. (2015). *Chechnya’s Terrorist Network: The Evolution of Terrorism in Russia’s North Caucasus*. Santa Barbara, CA: ABC-CLIO.

Raab, J., and Milward, H. B. (2003). “Dark Networks as Problems.” *Journal of Public Administration Research and Theory* 13(4): 413–439. doi:10.1093/jpart/mug029.

Reed, T. C., and Stillman, D. B. (2009). *The Nuclear Express: A Political History of the Bomb and Its Proliferation*. Minneapolis, MN: Zenith Press. .

Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press. .

Schlumberger, G., and Gruselle, B. (2007). “For a Consistent Policy in the Struggle against Proliferation Networks.” Foundation pour la Recherche Strategique. .

Spindel, J. (2015). “Logistics of Ballistics: Power and Politics in the Global Missile Network.” Political Networks Workshops & Conference 2015. .

Suchman, M. C., and Eyre, D. P. (1992). “Military Procurement as Rational Myth: Notes on the Social Construction of Weapons Proliferation.” *Sociological Forum* 7(1): 137–161. doi:10.1007/BF01124759.

Thurner, P. W., Schmid, C., Cranmer, S., and Kauermann, G. (2015). “The Network of Arms Transfers 1950–2013: An Application of ERGMs and TERGMs.” Paper presented at the Annual Political Networks Conference, Portland, OR.

Turbiville, G. H. 1996. *Weapons Proliferation and Organized Crime: Russian Military Dimensions*. Colorado Springs, CO: Institute for National Security Studies, U.S. Air Force Academy.

United Nations. (1997). “Report of the Panel of Governmental Experts on Small Arms.” UN Documents A/52/298. .

United Nations, Department for Disarmament Affairs Staff. (2002). *The United Nations Disarmament Yearbook*. Vol. 27. New York: United Nations Publications.

United States Department of Defense. (2014). “Department of Defense Strategy for Countering Weapons of Mass Destruction.” Office of the Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction. .

United States Department of State. (2015). “World Military Expenditures and Arms Transfers.” .

Valencia, M. J. (2007). “The Proliferation Security Initiative: A Glass Half-Full.” *Arms Control Today* 37(5): 17–21.

Ward, M. D., Ahlquist, J. S., and Rozenas, A. (2013). “Gravity’s Rainbow: A Dynamic Latent Space Model for the World Trade Network.” *Network Science* 1(1): 95–118. doi: 10.1017/nws.2013.1.

Ward, M. D., and Hoff, P. D. (2007). “Persistent Patterns of International Commerce.” *Journal of Peace Research* 44(2): 157–175. doi:10.1177/0022343307075119.

Willardson, S. (2013). “Under the Influence of Arms: The Foreign Policy Causes and Consequences of Arms Transfers.” PhD thesis, University of Iowa. .

Williams, Phil. (2001). “Transnational Criminal Networks.” In *Networks and Netwars*, edited by J. Arquilla and D. F. Ronfeldt, pp. 61–97. Santa Monica, CA: RAND Corporation.

Notes:

([1]) SALW are “those weapons designed for personal use, and light weapons are those designed for use by several persons serving as a crew” (United Nations, 1997, 11); WMD are “chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties, excluding the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon” (United States Department of Defense, 2014, 17–18); MCW constitute everything in between (aircraft, armored vehicles, missile systems, etc.).

([2]) In the literature, “proliferation networks” generally refer to WMD or related delivery methods, “arms trade networks” to MCW, and “illicit arms trade” typically to SALW, although any of these terms might apply to the others. We follow this convention here, being specific wherever possible and referring to “arms transfers” when referring to the general phenomenon.

([3]) The most relevant extant case here is still the Chechen placement of radiological materials and dynamite in a Moscow park in 1995. Although it is still unclear where material came from, it is likely it was acquired internally by the Chechens. See Pokalova (2015, 51).

([4]) It is still unclear whether A. Q. Khan or his organization was acting with the knowledge of the Pakistani government, but either possibility is bad: either nonstate entities can proliferate without governmental knowledge, or the government was actively supporting proliferation (thanks to Scott Sagan for this observation).

([5]) Originally called *World Armaments and Disarmament*, the SIPRI yearbook has been published since 1969. Current and past data can also be retrieved from the SIPRI Arms Transfers Database online at www.sipri.org/databases/armstransfers.

([6]) There are two other commonly used sources of quantitative information on conventional arms transfers. The US Department of State’s Bureau of Arms Control,

Verification and Compliance (AVC) releases *World Military Expenditures and Arms Transfers* (*WMEAT*), which includes annual bilateral arms flows, are most useful for network analysis, but only from major suppliers (United States, France, Germany, Italy, United Kingdom, Russia, and China). The data are available online at www.state.gov/t/avc/rls/rpt/wmeat/ (United States Department of State, 2015). The Congressional Research Service (CRS), a research arm of the US Congress, also publishes arms trade data in its periodic report *Conventional Arms Transfers to Developing Nations* (e.g., Grimmett and Kerr, 2012). These data are limited to transfers by major suppliers to developing countries only, but are noteworthy for distinguishing between arms agreements and arms deliveries.

([7]) States are invited to provide information on their conventional arms transfers for the UN Register of Conventional Arms, and although the UN register originally recorded only major weapon transfers, nearly sixty states have now provided information on their SALW transfers as well. This reporting is completely voluntary, however, and it is clear from the database that only a fraction of SALW exports and imports have been recorded. See Holtom (2009) and United Nations, Department for Disarmament Affairs Staff (2002).

([8]) Much of the data compiled and distributed by both the Small Arms Survey and NISAT are drawn from customs information in the UN's Commodity Trade Statistics Database (Comtrade). The NISAT Small Arms Trade Database can be accessed at nisat.prio.org/trade-database/, and visual maps of the data are available at nisatapps.prio.org/armsglobe/index.php. Other SALW data are collected by the Small Arms Survey, located at the Graduate Institute of International Studies in Geneva. The Survey's staff conducts in-depth country studies and other analyses focusing on various dimensions of legal and illicit SALW, many of which are reported in its annual review along with limited amounts of quantitative data. This information is available at www.smallarmssurvey.org/?small-arms-survey-2015.

David Kinsella

Division of Political Science, Portland State University

Alexander H. Montgomery

Department of Political Science, Reed College