Crime, Law & Social Change (2006) 45: 165–184
DOI: 10.1007/s10611-006-9033-5

Delivering security through networks: Surveying the relational landscape of security managers in an urban setting

BENOÎT DUPONT
University of Montreal

Abstract. The concept of network is fast becoming ubiquitous. Its broad appeal lies in its ability to account for the present multiplicity of institutional, organizational, and social morphologies. Networks promise to absorb, recombine, and merge the two dominant and competing forms of social organization (the bureaucratic hierarchy and the market) into a third one that would transcend the proclaimed obsolescence of bureaucracies (see for example Osborne and Gaebler, 1992) or the excesses of the market. Crime or dark networks (Raab and Milward, 2003) and their real level of (dis)organization have been studied for a number of years (Naylor, 2002; Morselli, 2005 and in this issue), but the 9/11 events and the failures of the vertical-hierarchical bureaucratic forms of security delivery they highlighted provided an audience to those advocating flatter and more flexible law enforcement assemblages (Williams, 1994; Arquilla and Ronfeld, 2001).

Police and private security organizations are quite familiar with the concept of network: they have embraced social network analysis to better understand the structure of criminal and terrorist groups and anti-fraud software that identify hidden patterns of collusion are routinely used by utilities companies and corporate security services. However, security organizations have been surprisingly slow to use these same tools to map their own policy and delivery environment. Academics have been more enthusiastic, but the few efforts so far to map existing security networks have either focused on a few nodes (Newburn, 2001; Cooley, 2005 for three Canadian case studies) or emphasized narrative and statistical data describing the roles of the various actors, their mandates, and their interests (Crawford et al., 2005; Fleming and Rhodes, 2005). Quantitative techniques have very rarely been mobilized in this area, despite a long sociological tradition of their use in social, organizational, and political network analysis (Knoke, 1990; Freeman, 2004). To date, and to the best of my knowledge, only one study (never cited in criminological works) has attempted to measure the role played by social capital in the recruitment strategies of the private security industry (Erickson, 2001). No such research has been carried out on the police. As a result, the concept of network is often used metaphorically, leading to various interpretations of what a network is, what its properties are, and what it does or even what it ought to be doing (Johnston and Shearing, 2003). This lack of empirical preciseness has led some to voice their scepticism about the network concept (Manning, 2005; Loader and Walker, 2006) to understand the current state of security delivery. While the network theoretical framework is no better equipped than the state or market paradigms were to account for the complexity of security authorization and delivery in modern (an not so modern) societies, it can still prove a useful tool in the methodological box at our disposal to grasp the complexity and multidimensional nature of this public good. Hence, this article seeks to illustrate how the development and analysis of detailed datasets on the relational landscape of security organizations and their managers can contribute to the growing literature on security networks.

This article introduces some considerations on the methodological tools that can be mobilized to map and model complex organizational sets. Some results these analyses can yield will also be discussed in order to illustrate how a more detailed knowledge of the transactions occurring in the security field can inform policy and guide state intervention. In order to provide a more concrete approach, I use data collected in a large city, ranking among the ten largest in North America for its population. The focus is mainly on the analysis of quantitative data, first by looking at the macro-structure of the network and then by detailing the micro-properties of the partnerships involved. The first part of this article clarifies the definition of networks that informs this approach, and describes their most salient properties in the security field. A second section examines the methodology that can be used to sketch security networks and their many dimensions empirically, as well as the challenges that must be overcome in order to do this. Finally, in the two final sections I provide some examples of how the data can be analysed and interpreted at the macro- and micro-sociological levels, suggesting that the notion of a *Securisphere* is more useful in understanding the authorization and delivery of security than the static idea of a state monopoly or the commodification thesis (Loader, 1999).

1. Defining security networks

The concept of network lends itself to a number of ambiguities that have contributed to its attractiveness and wide use in sociology, political science, and criminology circles. When the term is not used metaphorically,[1] researchers have often relied more on intuitions of what a network is or how it behaves than on the stimulating research that is available on the empirical features of social and organizational networks (for a small sample of this research, see for example Burt, 1992; Castells, 1996; Morselli, 2005; for a popular history of graph theory and network analysis see Barabási, 2002). Intuitive use of the term rarely differentiates between formal, informal, and technological dimensions and almost never considers the varied structures and substructures that can be found in a network, such as clusters, cliques, hierarchies, or random distributions of ties (Brodeur and Dupont, 2006). Imprecise use of the term allows it to be seen as analogous to communications or transport networks, evoking notions of highly coordinated assemblages. It is, however, easy to identify networks (in the sociological sense of the term) within groups of people or organisations that are not explicitly aware of the numerous and indirect links that bind them. This is especially true in the case of large-scale networks, where size obscures the structure, and in secret networks, whose survival depends on the compartmentalization of links (as in informant or terrorist networks).

It is clear that a precise definition of the concept of security network, and an explanation of its implicit boundaries, is needed. In this chapter a security network refers to a set of institutional, organisational, communal, or individual agents or nodes that are directly or indirectly connected in order to authorize and/or provide security for the benefit of internal or external stakeholders (Dupont, 2004; Shearing and Wood, 2000). The variety of nodes found in such networks is the source of structural heterogeneity and inequality (Castells, 2000:11): large government agencies and transnational corporations operate in the same field as local interests and family-owned businesses, with some entities made up of only one person (consultants, for example). Nevertheless, a complex web of recurrent interconnections and linkages brings these nodes together on a voluntary, contractual, or regulatory basis. One problem commonly found in network analysis is its failure to recognize the importance of determining node identities, thereby blurring the boundaries between nodes and their links. When a node reaches a certain size, it can be described as a network in its own right, which can create problems with using the concept. Consider, for example, the case of the U.S. Department of Homeland Security, which amalgamated 22 existing government agencies in one of the largest examples of bureaucratic restructuring in the US in the past 50 years. In its current form, the level of fragmentation and competition between sub-units makes it possible to consider the new entity an uncoordinated network (or dysfunctional hierarchy) (Carafano and Heyman, 2005). For methodological reasons, nodes in security networks will be considered to consist of organizations and individuals that operate as discrete entities and are viewed as such by the overall membership of the security field. This restriction is a simplification of reality, where, for example, the same organization can tap into networks through various different sub-units that promote various agendas. In other cases, an individual can represent more than one entity at the same time, for example as manager of a company and also president of a professional association. It is possible to compensate for these modelling limitations by collecting qualitative data that can more easily capture the nuances and meanings attached to particular nodes.

Security networks are formed around the authorization and delivery of security, through a range of processes and services that extend from the identification of needs and the resources available to respond to them, to the management of risks and the deployment of human and technological assets. Nodes can be specialized in the authorization or delivery aspects or can integrate both dimensions: while some businesses choose to outsource to private security companies, others prefer to develop in-house expertise. Security networks differ from the policy networks familiar to political scientists (Marsh, 1998; Rhodes this book), which are designed to shape policies around specific issues (at the sectoral or sub-sectoral levels). Although they may also be involved in policy debates, particularly around the nature and level of regulation, they are established and maintained largely within the context of routine activities associated with the production of security. The need to reduce exposure to uncertainty and contingency is also a strong incentive for belonging to a security network. The terms of exchanges between members of a security network are then guided less by the need to influence government decisions than by the capacity to pool resources in order to increase effectiveness and decrease vulnerability. There is no shared overall objective or value but instead a myriad of overlapping interests brought together by informal, voluntary, contractual, or regulatory ties. In this respect security networks are very similar to the large social and economic networks discovered by mathematicians and sociologists, which are not designed from the top but emerge progressively from regular interactions between their members.[2] The size of such networks and their multi-layered properties often limit members' awareness of the degrees of connection and interdependence within the network. In fact, just as M. Jourdain in Molière's play had been speaking prose for 40 years without knowing it, many nodes are indifferent to their whole security network, focusing their attention instead on the most proximate (geographical or relational) and regular contacts. Security networks are more incidental than teleological and, as such, their normative potential is dependent on a much more detailed understanding of their dynamics than the current metaphorical use of the term allows.

Because networks can potentially include a limitless number of actors through interconnection (the famous six degrees of separation theory), networks whose boundaries are not carefully defined quickly become impractical for empirical study, due to their exponential growth. Such networks are part of the work of mathematicians and physicists, who can develop simulations involving millions of nodes, but are much less practical for social scientists, who are confronted with the colossal task of collecting data in the real world.

Typologies can also be used both to clarify the area to be studied and to introduce some degree of scale to the study of networks. One useful variable to consider is the geographical scope of a network's mode of exchange: from the local to the international, through the national. We can reasonably expect security networks that operate at the local level to differ significantly in their membership and structure from national institutional networks and their international counterparts, which are concerned largely with transnational organized threats (Dupont, 2004). Social and organizational networks have also benefited from the development of technological or informational networks (Castells, 1996; Arquilla and Ronfeldt, 2001). However, even if these two kinds of networks are intricately integrated, they should not be expected to operate in the same way. As a few observers have already noted, the fact that data or information is available to a network is not in itself a sufficient condition to ensure its diffusion and use by all institutional nodes. Social processes similar to those that facilitate the creation and transfer of tacit knowledge (Polany, 1967; Nonaka and Takeushi, 1995; Brown and Duguid, 2000) can block the circulation of explicit knowledge within a security network (NCTAUS, 2004; Sheptycki, 2004).

Obviously the tentative typology presented here does not preclude overlaps and connections between categories. Nor does it necessarily capture all the relevant and significant variables of security networks, whose complexity challenges any analysis that relies exclusively on theoretical tools.

2. Network mapping methodology

In order to capture the essence of security networks, extensive data must be collected about the nodes they are composed of and the properties of these nodes, as well as about the webs of linkages that bind nodes together. There is a growing body of statistics that attempts to measure the size of the private security sector in terms of employee numbers (Prenzler and Sarre, 1998; De Waard, 1999) and is then used to design crude indicators such as the ratio of private to public security employees. Such indicators are useful to chart the diffusion of responsibilities in the security field – what Bayley and Shearing (2001) call the multilateralization of security – but, although these methods are useful in assessing the size of the submerged part of the security iceberg, they cannot tell us who is doing what, with whom, and how frequently. Any methodology we develop must fill this gap.

The amount of data required and the resources available for this research led me to limit this work to the geographical area of a large metropolitan centre of 1.8 million people. This city covers an area of 500 square kilometres, and had an estimated GDP of USD100 billion in 2003. 28% of its population are immigrants, and the unemployment rate is 9.2%. 50% of the inhabitants have a college or university degree. In 2004 the annual city budget was USD3.15 billion, 18.7% of which was spent on public security. One of its features is a 30 km underground network of public and private pathways that connect 10 subway stations, 2 bus terminals, 2 train stations, 4 universities, 10 cinemas and theatres, 200 restaurants, 1,600 apartments, 1,700 retail stores, and 80% of the city's office spaces. Each day, half a million people use this network. This web of private properties (Shearing and Stenning, 1981) provides a powerful incentive for public and private security nodes to coordinate their activities in order to prepare for emergencies and prevent some forms of criminal activity.

The nodes of this local security network were defined as public and quasi-public organizations involved in the production of security, in-house (proprietary) security services for industrial or service oriented businesses, and private security companies. Nodes were thus defined as entities or segments of entities whose primary function is the authorization and/or delivery of security for communities, individuals, and organizations residing, working, studying, shopping, consuming services, or producing goods in this large metropolitan area. Relevant entities were formally identified through membership lists of the two main professional security associations active at the local level, the latest registration data of the regulatory body in charge of private security, the yellow pages of the telephone book, and snowball sampling during the collection itself. One difficulty with this way of 'counting' the nodes is that it does not take into account variations in terms of size. A small number of nodes (such as the public police and large private security companies that employ thousands of workers) account for most of the workforce, while a large number of nodes are composed of only a few employees. In this respect, the impact certain organizations have on the field has nothing in common with the light footprints left by others. This inequality is reflected, to a certain extent, in the distribution patterns of ties – and power or influence are not, of course, exclusively derived from size. It is nevertheless important to remember that the visualization tools used in network analysis have a tendency to discard many node properties in their representations, and that two very different nodes might end up looking the same on a diagram.

Data was gathered through interviews with each node's manager and covered the formal and informal dimensions of existing partnerships. The choice of managers as the primary respondents introduces some limitations, as they are unlikely to be aware of all the ties their employees maintain with colleagues in other nodes. However, their decisions are more likely to result in policy and practical changes, and as a result to affect the structure of the field than those made daily by frontline workers, whose practices are more routine

(Erickson, 2001). Managers can thus provide a satisfactory overview of the more important ties. Exceptions were made for larger and more complex organizations such as the police, whose division of labour and long hierarchical chain require access to more than one respondent in order to map the numerous linkages activated daily. In those cases, key informants from various units of the organization were interviewed. The interviews consisted of a qualitative component, which attempted to establish a profile of the node in terms of tasks accomplished, resources, expertise, and governance structure, and a quantitative component, which took the form of a multi-variable contact matrix. Each respondent was given a ‘node generator’, a constantly updated list of all the nodes in the security field under study.[3] Respondents were asked to name the nodes with which formal and informal ties had been maintained over the past twelve months. Because of the exploratory nature of this research, questions about ties were deliberately framed in the most general terms in order to include the many forms of partnerships and exchanges that might occur. (Future research should involve more detailed questionnaires that can discriminate between various layers of linkages by nature or perceived usefulness). For each contact, respondents were asked to specify nine variables:

- The number of individual contacts within the partner organization
- The existence of more privileged relationships with one of these contacts
- Extra-professional socialization with those contacts
- The context in which meetings with professional contacts occur outside the workplace (friendship, kinship, love affair. . .)
- The frequency of contacts with the privileged partner or the group of contacts
- The general distribution of responsibilities for activation of ties
- The preferred technological tools used to interact with the contact
- The contact’s perceived level of responsibility (as compared to the respondent)
- The formal or informal nature of the partnership

There were a number of challenges associated with collecting the data. The decision to complement quantitative data with qualitative data and the repetitive process of going through nine variables for each recorded contact made data collection time-consuming in a context where respondents had extremely busy schedules and unexpected circumstances often delayed the arranged interviews. Nevertheless, 50 respondents were interviewed over a period of 16 months, from January 2004 to April 2005. The breakdown of their organizational affiliation is provided in Table 1.

Unless the network we are studying is randomly structured, the sampling strategies used in statistical analysis cannot be applied. Ideally, mapping a

Table 1. Respondent's organizational affiliation

	N	%
Public police	4	8%
Hybrid sector	23	46%
Professional associations	1	2%
In house (proprietary) private sector	14	28%
Contract generalist	3	6%
Contract investigations and expertise	3	6%
Contract equipment	2	4%
Total	50	100%

network should include identification of all its components, because we are trying to measure inconsistencies (the extreme values are the most significant). Considering only a sample of the components might miss a key node of the network, even, perhaps, the 'hub' that allows the network to function properly. Relying exclusively on snowball sampling or other self-selection methods such as membership lists runs the risk of mistaking a sub-component (albeit a large one) for the whole of a network. Unfortunately real-life networks are sprawling and may include large numbers of nodes which can be catalogued only by reducing data thickness. In our case, for example, the 207 nodes listed by our 50 respondents certainly did not include all actors in the city's security system. However, the high density and connectivity uncovered, coupled with the fact that the data originated from diversified nodes, make it unlikely that key parts of the local network were omitted. Compromises and an element of arbitrary judgment are unfortunately unavoidable when partitioning a network (deciding where it ends for the purpose of the study). The fact that networks have quasi-organic properties also represents a challenge for the researcher. During the study a few respondents accepted new responsibilities with other nodes, others were demoted or lost their position through downsizing. This constant evolution of networks (including possible collapse) is invisible in the snapshots provided through the tools used here, but more recent methodological developments add a temporal dimension to the mapping of nodes (Powell et al., 2005).

The collected data was imported into two distinct software packages: Ucinet, a social network analysis package that performs basic operations such as measurement of centrality, subgroup identification, role analysis, and elementary graph theory routines (Borgatti et al., 1999); and SPSS, which was used to perform basic statistical analysis of tie variables.

3. The structural properties of a security network

The respondents belonged to 47 discrete organizations,[4] which taken together, employ 17,480 people[5] and provide security as a public service, internally, or on contract. (This last category includes the municipal police service with its 3,900 officers, a few large private security companies that offer guard services and employ more than 1,000 people, and a large majority of in-house or for-contract security organizations that rarely have more than 100 employees). As I will show below, these respondents are embedded in a broader network of security nodes, but they constitute a representative sample of the various organizations encountered, based on their respective sizes and the distribution of their responsibilities. The average length of respondents' experience in the security field was 19.75 years (median: 20 years; std. deviation 12.16), including experience acquired in the public police by those who had started a second career in private security. This group, whose expertise and contacts were transferred from the public to the hybrid or private sectors, has often been described as the 'old boy network'. It accounted for 26% of the respondents and its members can be found mainly in two categories of organizations: hybrid para-public organizations and in-house security of large companies. Very few of these individuals chose to join the generalist, investigation, or technology-related private security companies.

Despite the fact that respondents used the generic term 'security' to describe what they were doing, a diversity of meanings, rationalities, and outcomes is associated with the processes of authorization and delivery. If the consensus around the police mandate is that it authorizes the use of coercive force when needed to maintain order and enforce the law on behalf of all citizens, hybrid and private security nodes are more inclined to work proactively to manage risks and cannot mobilize extensive – and legal – force to achieve that end. In the case of mass private properties (Shearing and Stenning, 1981), the risks to be managed are mainly those that threaten the routine activities of customers or users, while manufacturing or high tech companies are more concerned with the integrity of their assets (such as intellectual property or costly equipment). The financial and governmental sectors emphasize the reliability of their procedures and want to make sure that these are not compromised by fraudulent behaviours, and that when it happens, these events remain unknown to the public. Each actor, depending on the sector of activity and the demands of its stakeholders, develops a distinctive form of expertise, suited to its resources and constraints. One privileged strategy for significantly enhancing the quantity and quality of resources and lowering the impact of external constraints is to resort to partnerships. These partnerships, formal or informal, represent the 'bones' of the network. They can involve

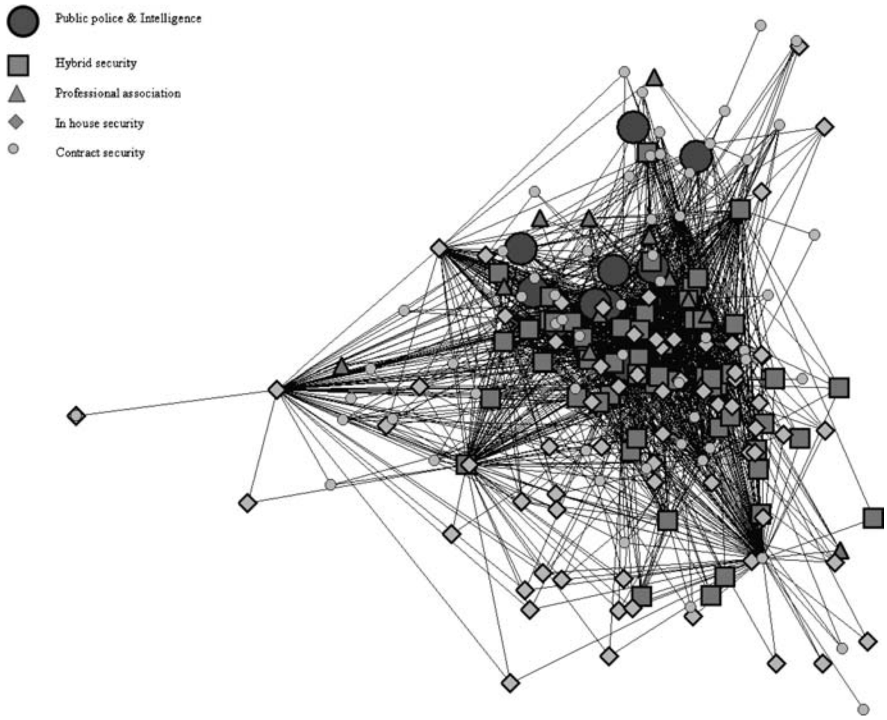

Figure 1. Complete network (Gower).

the exchange of information about threats, best practices, potential providers, clients or employees; the pooling of resources such as CCTV feeds; the joint management of training programs; or the implementation of new standards of practice. Figure 1represents the patterns of partnership revealed by the 47 security nodes we interviewed, which declared an overall network of 207 organizations operating in their immediate environment (due to the density of the network and the ties, a few nodes might be superimposed). Each line represents a partnership that was active over the previous twelve months.

The intricate network pictured in Figure 1, which resembles a bird's nest, represents only a fraction of all potential ties between the 209 organizations, 23% to be exact. In order to properly measure the characteristics of the network, it was necessary to restrict the analysis to nodes that provided us with their complete list of partners and for which we had reciprocal data. The core network of interviewees, represented in Figure 2, has an average density of 46%, meaning that 46% of all possible partnerships between nodes are considered to be active. This is quite high given the number of organizations being considered and their heterogeneity. This high density is confirmed by the high connectivity of the network: when we compute the distance between nodes,

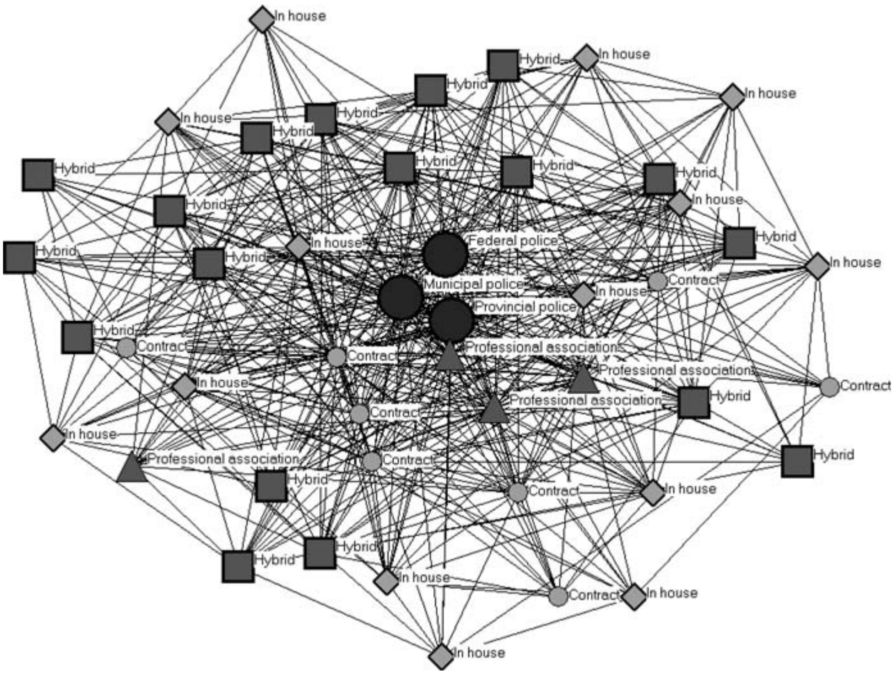

Figure 2. Core network (spring embedding).

we see that the average geodesic distance is 1.5, which implies that actors can reach all the other nodes of the network through only one intermediary (this would be the shortest path, but many more less efficient connections could be made). In such a tightly knit environment, where many alternatives to reach the same person are available, information travels fast and is easy to retrieve, exchange costs are relatively low, and new trends will be adopted rapidly. Reputations, which can be undone at a fast pace, become a valuable asset and everything will be done to maintain them.

Another essential dimension in network analysis is centrality, which illustrates the distribution of power within a network: the more central a node's position, the more opportunities it will have, the fewer constraints it will experience, and the more influence it will derive from its position. The amount of power derived from centrality also depends on the density of the network, but the two are not systematically correlated: dense networks can be highly centralized around a dominant player, but they can also be structured with a cliquish distribution of power, meaning that denser sub-groups loosely connected to each others will emerge. In the field of security, the public police is without any doubt the hub to which all actors converge because of its control over two essential assets: the legitimate use of force and the legal access to identity and crime-related information. But the core of the network is not the exclusive domain of the police: professional associations also play a central role. They provide continuing training to their members and allow them to tap into a vast reservoir of expertise. They are also a privileged marketplace where technology and service vendors meet prospective customers and where potential buyers can check the credentials of existing providers with their former or current clients, who attend the same meetings.

One striking aspect of this core is the fact that it is made up of two very loosely linked components: very few police respondents mentioned formal or informal ties with professional associations and the representatives of those associations lamented the lack of interest on the part of the police. Only a few hybrid organizations were members of the provincial association of chiefs of police, included apparently because of their limited legal powers to investigate or their mandate to act in the public interest (such as overseeing the security of an international airport). The police and professional associations seem to be less likely connected to each other than to the rest of the network and to engaged in an implicit competition – albeit with different resources at their disposal and different costs incurred – for the central role in the overall network. While the police officers interviewed had a lower-than-average number of ties outside the public police sector and appeared to be comfortable with this situation, their organization is the largest 'sink' of partnerships in the network, with 96% of nodes stating that they maintained a link of some sort with the municipal police. The percentage of those with links to the provincial and federal police, whose jurisdictions are more narrowly defined is marginally lower (87% and 83% respectively). By way of comparison, the average for the non-police members of the network was 29%. The legitimacy of the police, confirmed by the efforts of all other actors to maintain a privileged relationship with it, is in sharp contrast to the more laborious process of expertise exchange and certification offered by professional associations. Professional associations were constantly involved in recruitment drives and initiatives that would keep their members coming back and operate in a highly competitive environment.

In both groups, less powerful members sought ways to reduce constraints and exposure to external contingencies. This is the reason nodes maintain numerous transversal ties, which avoid excessive dependence on the centre and permit them to hedge their exposure to risk in case of an emergency. When police organizations and professional associations are removed from the matrix before connectivity tests are run, the average distance between two nodes remains constant at 1.6 (remember it was 1.5 for the complete network). This indicates an absence of decay: the network is still active and can operate effectively without its core, even if efficiency decreases slightly because fewer options are available. The network clearly acknowledges the power and authority of the police, but it does not depend on it to mediate its exchanges on a routine basis, as many security partnerships are built around the police.

The existence of many cliques or subgroups where members' ties with each other are stronger than with the rest of the network[6] attests to this lack of dependence on the police. In our dataset, there are 247 cliques of 7 nodes or more and 78 cliques of 10 nodes or more. As would be expected, there is a large degree of overlap between these denser sub-groups, corresponding to functional or personal affinities: the heads of security for educational and cultural institutions share common problems and therefore exchange more information more frequently, as do their public transport counterparts or any particular subset of security providers. In our interviews the banking sector, the high tech industry (aerospace, pharmaceutical), large retail malls, hospitals, and public transport entities tended to exchange information and resources more intensely, sometimes creating their own specialized association or seeking privileged linkages with counterparts at the national or international levels. Clusters of exchanges can also form along geographical lines, such as a large subway station located within a university campus, itself surrounded by the red light district, or the interconnected system of underground retail spaces and high-rise office towers, where millions pass seamlessly every year, oblivious to the coordinated security grid humming in the background. Finally, the personal experiences of the members of a node are defined to a certain extent by the radius and nature of their relational neighborhood. One example should be sufficient to illustrate this point. Among the five university security chiefs interviewed, the size of the immediate network varied from 10 to 28 partners. The size of the institutions they worked for and their mandates were relatively identical but their professional trajectories differed greatly. One of them is a retired police officer who has also tried his hand at security consulting, while others are general managers who have no prior experience in security and do not plan to stay involved in it as a long-term career. They therefore come to the position with little specific social capital and do not invest heavily in new partnerships beyond those that are essential.

Cliques, whether based on functional, geographic, or personal dimensions, mobilize varied levels of trust and reciprocity to function. While superficial trust is sufficient for the overall network to operate, resilient trust is necessary at the subset level (Smith Ring, 1997). This stronger form of trust is reinforced through frequent exchange of favours and displays of accommodating behaviours, which must be bidirectional. The equilibrium, however, is fragile and some dominant players may attempt 'hostile takeovers' of weaker nodes. For example, the municipal police force recently encouraged a carefully orchestrated campaign in the media to discredit the special constable subway force by leaking statistics that showed higher-than-average crime rates in subway stations. As a result of this campaign, the police managed to absorb subway security, effectively extending its reach to the underground city – and probably making other public transport security providers nervous.

If a shared set of occupational values acquired in an earlier career can come in handy at times, membership in the 'old boy network' is not sufficient to secure a management position in the hybrid and private security sectors. More than law enforcement skills *per se,* what is valued and transferable from police organizations to the broader network is a well-filled address book and direct access to specialist units. Furthermore, the development of university courses in the field of security (at the bachelor level or in the context of continuing education) is creating a growing number of candidates whose academic qualifications are gradually being considered relevant and who are likely to form cliques of their own as a defensive (or offensive, depending on the perspective) strategy to ensure that they quickly access the managerial positions at the core of the network.

The security network depicted here is the result of the amalgamation of many smaller overlapping organizational and personal subsets of relationships, whose common denominator is the authorization and delivery of security in the most general definition of the term. The multiplexed nature of this network is expressed through varied levels of cooperation, competition, trust, and reciprocity but provides the institutional fabric of urban security. In this sense, the term network is used to describe a multi-dimensional set of interactions and interdependencies. The neologism of *Securisphere* might actually be a more appropriate name for the institutional space within which security is produced and, by extension, for the actors that fill it, their fluid partnerships, and the security deficits that develop through negligence or lack of coordination. The term emphasizes the emergent properties produced by the interactions and interdependencies of nodes or, stated more simply, what transcends the sum of all parts. One intangible manifestation of these emergent properties is the trust and reciprocity that are instrumental in achieving collective outcomes: take for example the case of a subway station located within a university campus where frequent political demonstrations spill over on the crowded streets in its vicinity. When good relationships exist between the campus police, subway security and the municipal force, coordinated responses to equipment theft, vandalism and potential disruptions to public order deliver positive impacts that cannot be broken down according the measurable contribution of each partner. The trust that binds them together (and can be generated by a range of processes) is also a significant factor that is rarely taken into account.

Table 2. Number of mean ties by respondent's sector of activity

	N	Mean	Std. Dev.
Public police	4	9	7,05
Hybrid sector	23	30	19,77
Professional associations	1	64	–
In house (proprietary) private sector	14	36	14,89
Contract generalist	3	30	43,04
Contract investigation and expertise	3	31	12,29
Contract equipment	2	104	22,63
Total	50	34,78	24,73

4. Building trust: The power of reciprocating ties

A micro analysis of the ties that connect the members of the network will help clarify the various relational profiles found among security managers. Our 50 respondents declared an average of 34 ties per node (range: 2–120). However, depending on the sector of activity of the node, the average number of contacts ranges from 9 in the case of the police to 104 in the private technology sector (see Table 2).

The low number of contacts maintained by police officers can be explained by their central position, in which they are more in demand than in search of contacts, but also by the size and specialization of their organization, which allows a broader distribution of incoming and outgoing linkages. The contract technology sector displays an unusually high number of contacts, reflecting their constant need to find new clients and the ferocious competition in this field where investments are booming and innovations are constant – an interpretation confirmed by the fact that respondents declared an average of 3.5 technology providers, with high rates of turnover. When we plot the distribution of our sample according to the number of partners declared (the size of each respondent's personal network, also known as degree distribution), the shape of the curve (Figure 3) produces a peak culminating in the vicinity of 30 partners, followed by a long tail indicating a slow decay, with a few organizations declaring more than 80 contacts (see Figure 3).

The frequency with which these contacts were activated (the rate of communications between the nodes for a twelve months period) did not follow a predictable pattern, with a median of 21 interactions per year (range 4.4–307). The broad distribution seems to confirm the multiplex nature of the ties. The flows of communication these numbers reveal add a layer of intensity to the density already uncovered in the previous section: this

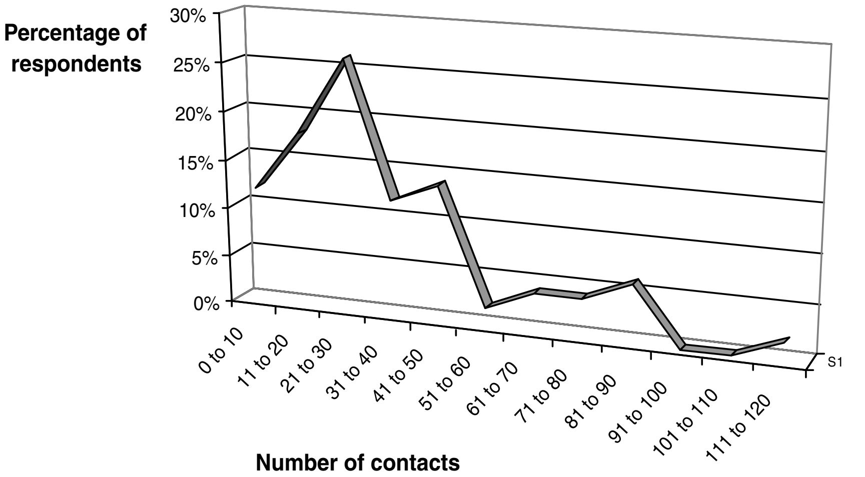

Figure 3. Distribution according to number of contacts.

network is characterized by a regular monitoring of changes and responds accordingly to needed adjustments.

These partnerships are based on individualized contacts, with 81% of the respondents having privileged access to three persons or fewer in the partner organizations and 52% having a sole point of entry. This dependence on a few individuals to keep partnerships alive is both a source of strength and a potential weakness. The personalized contacts are beneficial to the development and reinforcement of resilient trust but can also undermine – or at least temporarily disable – existing relationships when a member leaves his/her organization. It should therefore not come as a surprise that replacements must often demonstrate their "trust-ability" through a certifiable amount of social capital (Erickson, 2001).

The importance of trust is also shown through an assessment of hierarchical equivalence between partners: 61% of contacts were believed to have responsibilities similar to those of respondents, a clear sign that a majority of lasting partnerships involve equals, whose trust rests on a shared body of experiences and preoccupations. This perceived egalitarian feature of the network is confirmed by answers to questions that measure dependency toward other nodes: 40% of contacts were described as the result of equal initiatives, and 20% were derived from demands of the partner, while 40% follow a request of the respondent. This relatively balanced distribution suggests a level of exchange reciprocity that fosters trust. The 15% of contacts reported as being located higher in the network hierarchy provide more sporadic strategic advice, information, or support, but their impact is, of course, incommensurable with the frequency of contacts. Contrary to what was expected, little socialization seemed to take place other than at work-related events such as conferences, golf tournaments, and industry banquets. Only 8% of our respondents stated that they maintained ties with their contacts outside the professional realm.

These preliminary results should be interpreted with Nadel's paradox in mind: while structural modelling allows us to study and compare networks systematically, each node – or even the employee of a node – will nevertheless act according to a unique understanding of the network's membership, constraints, and utility (Nadel, 1957; DiMaggio, 1992; Berry et al., 2004). No analysis of such complex phenomena should rest exclusively on quantitative data, as it would invariably be prone to incomplete interpretations.

5. Conclusion

Notwithstanding its primary functions of law enforcement and order maintenance, public policing is embedded in a broader security network, which it helps to shape (both intentionally and incidentally) but which also develops its own answers to the problems of crime, insecurity, and safety. This is of course not a new finding, but the asymmetrical pattern of linkages between the police and other security providers is more intriguing: the lack of reciprocity from the police to the very deliberate partnership strategy of the private and hybrid sector can be interpreted as the exploitation of public resources for the benefit of private interests. In a period of fiscal constraint, one might question the extent to which private security providers seem to mobilize public policing in furtherance of their own ends, in a context where the police seems indifferent or unable to harness with the same efficiency the power of networks.

The empirical contribution made by this article could complement the growing body of theoretical literature on the pluralization of security in two different ways. First, it introduces a dose of reality – and messiness – which tends to be easily 'forgotten' in our attempts to put forward elegant and neat explanatory frameworks. The proposed artificial opposition between those who refuse to concede that state monopoly over the authorization and delivery of security is weakened, on one hand, and those who preach the gospel of the market, on the other, is an oversimplification of the much more intricate blend of arrangements that often materialize in an *ad hoc* fashion (see for example the case studies in Manning, 2006). Second, they provide some tools that allow us to capture the essence and constants of this complexity (within the limits stated above) and can support more appropriate normative frameworks that take advantage of the nodal properties highlighted above.

More concretely, this methodology could be used to assess the relevance of current internal and external oversight mechanisms, and to explore the potential of meta-regulation (Parker, 2002; Braithwaite, 2003) to better ensure the just and equitable distribution of security. Are there security holes or deficits in the *Securisphere* that need to be filled? Can certain groups of individuals or corporations hoard publicly and privately produced security, leaving others deprived of this essential collective good? Another preoccupation is the ability of security networks to evade accountability requirements. By facilitating the offloading of certain tasks to other nodes of the network which are under lower levels of scrutiny, do security networks undermine democracy by diluting the effectiveness of mono-institutional control mechanisms? In the domain of high policing, the case of the torture network established by the US government and some of its close allies in the so-called War against terrorism (Marty, 2006) represents an example of security networks', detrimental potential. The question of coordination should also be examined in greater detail: to what degree can security networks be coordinated, and what mechanisms are best suited to provide the optimal level of collaboration? Should a single node be given the mandate for this role? Should encouraging coordination be a task given to an existing node or do we need to design a new type of governing institution that is more appropriate for the pluralized structure of security delivery? The methodological challenges alluded to earlier in this chapter are likely to translate into equally complex normative challenges, as networks are much harder to assemble and to steer than the vertical bureaucracies with which we are familiar.

Notes

1. This metaphorical usage is often unintentional.
2. For an example of a network simulation involving more than a million and a half nodes and concerned with the transportation and health patterns of a large urban area, see Barrett et al. (2004).
3. However, all the respondents in the sample were included in the initial list and the additional nodes are only located in the periphery of the full network.
4. Open source data (memoranda of understanding and joint operations) and confidential membership lists (in the case of professional associations) were also used to complete the contact matrix, which explains why a few nodes are represented without a formal interview. In those rare cases, no data other than the existence of a partnership could be collected.
5. Special care was taken to avoid double-counting of employees provided by security companies to guard the premises of clients who also had their own in-house security detail. However, this was possible only to the extent that information provided by our respondents was accurate.
6. A clique is defined as a group with a complete set of ties, or one where all nodes are connected to all others. Thus, the density of a clique is 100%.

References

Arquilla, J. and D. Ronfeldt (eds), *Networks and Netwars* (Rand, Santa Monica, 2001).

Barabási, A.-L., *Linked: The New Science of Networks* (Perseus Press, Cambridge, 2002).

Barrett, C.L., S. Eubank, V.S. Anil Kumar and M.V. Marathe, "Understanding Large Scale Social and Infrastructure Networks: A Simulation-Based Approach," *SIAM News*, 2004 (37:4), 1–5.

Bayley, D. and C. Shearing, *The New Structure of Policing: Description, Conceptualization and Research Agenda* (National Institute of Justice, Washington DC, 2001).

Berry, F., R. Brower, S. Ok Choi, W. Xinfang Goa, H. Jang, M. Kwon and J. Word, "Three Traditions of Network Research: What the Public Management Research Agenda Can Learn from Other Research Communities," *Public Administration Review*, 2004 (64:5), 539–552.

Borgatti, S.P., M.G. Everett and L.C. Freeman, *UCINET 6. Version 6.59* (Analytic Technologies, Natick, 1999).

Braithwaite, J., "Meta Risk Management and Responsive Regulation for Tax System Integrity," *Law and Policy*, 2003, (25), 1–16.

Brodeur, J.-P. and B. Dupont, "Knowledge Workers or 'Knowledge Workers'?" *Policing and Society*, 2006, (16:1), 7–26.

Brown, J.S. and P. Duguid, *The Social Life of Information* (Harvard Business School Press, Boston, 2000).

Burt, R.S., *Structural Holes* (Harvard University Press, Cambridge MA, 1992).

Carafano, J. and D. Heyman, *DHS 2.0: Rethinking the Department of Homeland Security* (The Heritage Foundation and Centre for Strategic and International Studies, Washington DC, 2005).

Castells, M., *The Rise of the Network Society* (Blackwell, Oxford, 1996).

Castells, M., "Materials for an Exploratory Theory of the Network Society," *British Journal of Sociology*, 2000 (51:1), 5–24.

Cooley, D. (ed.), *Re-Imagining Policing in Canada* (University of Toronto Press, Toronto, 2005).

Crawford, A., S. Lister, S. Blackburn and J. Burnett, *Plural Policing: The Mixed Economy of Visible Patrols in England and Wales* (The Policy Press, Bristol, 2005).

De Waard, J., "The Private Security Industry in International Perspective," *European Journal on Criminal Policy and Research*, 1999 (7), 143–174.

DiMaggio, P., "Nadel's Paradox Revisited: Relational and Cultural Aspects of Organizational Structure," in N. Nohria and R.G. Eccles (eds.), *Networks and Organizations: Structure, Form, and Action* (Harvard Business School Press, Boston, 1992), pp. 118–142.

Dupont, B., "Security in the Age of Networks," *Policing and Society*, 2004 (14:1), 76–91.

Erickson, B.H., "Good Networks and Good Jobs: The Value of Social Capital to Employers and Employees," in N. Lin, K. Cook and R.S. Burt (eds.), *Social Capital: Theory and Research* (Aldine de Gruyter, New York, 2001), pp. 127–158.

Fleming, J. and R. Rhodes, "Bureaucracy, Contracts and Networks: The Unholy Trinity and the Police," *The Australian and New Zealand Journal of Criminology*, 2005 (38:2), 192–205.

Freeman, L.C., *The Development of Social Network Analysis* (Empirical Press, Vancouver, 2004).

Johnston, L. and C. Shearing, *Governing Security: Explorations in Policing and Justice* (Routledge, London, 2003).

Knoke, D., *Political Networks: The Structural Perspective* (Cambridge University Press, Cambridge, 1990).

Loader, I. and N. Walker, "Necessary Virtues: The Legitimate Place of the State in the Production of Security," in J. Wood and B . Dupont (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge, 2006), 165–195.

Loader, I., "Consumer Culture and the Commodification of Policing and Security," *Sociology*, 1999 (33:2), 373–392.

Manning, P.K., "Two Case Studies of American Anti-Terrorism," in J . Wood and B. Dupont (eds), *Democracy, Society and the Governance of Security* (Cambridge University Press, Cambridge, 2006), 52–85.

Manning, P.K., "Some Notes on the Relationship of Private Security to Public Policing," Paper Delivered at the *First International Francophone Conference on Police and Citizens* (Nicolet, 30 May–2 June 2005).

Marsh, D., "The Development of the Policy Network Approach," in D. Marsh (ed.), *Comparing Policy Networks* (Open University Press, Buckingham, 1998), pp. 3–17.

Marty, D., *Alleged Secret Detention and Unlawful Inter-State Transfers Involving Council of Europe Member States* (Council of Europe Parliamentary Assembly, Strasbourg 2006).

Morselli, C., *Contacts, Opportunities and Criminal Enterprise* (University of Toronto Press, Toronto, 2005).

Nadel, S., *The Theory of Social Structure* (Cohen and West, London, 1957).

National Commission on Terrorist Attacks Upon the United States (NCTAUS), *The 9/11 Commission Report* (W. W. Norton and Company, New York, 2004).

Naylor, T., *Wages of Crime* (Cornell University Press, Ithaca, 2002).

Newburn, T., "The Commodification of Policing: Security Networks in the Late Modern City," *Urban Studies*, 2001 (38:5–6), 829–848.

Nonaka, I. and H. Takeushi, *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation* (Oxford University Press, New York, 1995).

Osborne, D. and T. Gaebler, *Reinventing Government* (Addison-Wesley, Reading, 1992).

Parker, C., *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge University Press, Cambridge, 2002).

Polanyi, M., *The Tacit Dimension* (Anchor Books, New York, 1967).

Powell, W., D. White, K. Koput and J. Owen-Smith, "Network Dynamics and Field Evolution: The Growth of Interorganizational Collaboration in the Life Sciences," *American Journal of Sociology*, 2005 (110:4), 1132–1205.

Prenzler, T. and R. Sarre, "Regulating Private Security in Australia," *Trends and Issues in Crime and Criminal Justice No. 98* (Australian Institute of Criminology, Canberra, 1998).

Raab, J. and H. B. Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory*, 2003, (13:4), 413–439.

Shearing, C. and P. Stenning, "Modern Private Security: Its Growth and Implications," in M. Tonry and N. Morris (eds), *Crime and Justice: An Annual Review of Research* (University of Chicago Press, Chicago, 1981), vol. 3, pp. 193–245.

Shearing C. and J. Wood, "Reflections on the Governance of Security: A Normative Enquiry," *Police Practice*, 2000 (1:4), 457–476.

Sheptycki, J., "Organisational Pathologies in Police Intelligence Systems," *European Journal of Criminology*, 2004 (1:3), 307–332.

Smith Ring, P., "Processes Facilitating Reliance on Trust in Inter-Organizational Networks," in M. Ebbers (ed.), *The Formation of Inter-Organizational Networks* (Oxford University Press, Oxford, 1997), pp. 113–145.

Williams, P., "Transnational Criminal Organisations and International Security," *Survival*, 1994 (36:1), 96–113.