*Policing & Society, Vol. 14, No. 1, March 2004, pp. 76–91*

Routledge
Taylor & Francis Group

# Security in the Age of Networks

Benoît Dupont

*Using the literature on the networked society as a starting point, this article argues that security can also be conceptualized as being produced by various networks of actors—public and private. This approach eschews the usual debate between those who defend the pre-eminence of the state (general interest) and those in favour of a plural mode of security production (market-oriented) to focus instead on the shared complex morphology that characterizes security assemblages in the present era: networks. Security networks are found in both Anglo-Saxon and Continental societies at the local, institutional, international and informational levels. In order to overcome the descriptive tendency of network approaches, a dynamic framework based on the capital metaphor shows how each actor of a security network mobilizes distinct forms of resources in order to maximize its position in the network. This framework can be applied to chart the emergence and transformation of security networks and the strategies deployed by their nodes.*

*Keywords: Security networks; Governance of security; Local security networks; Institutional security networks; International security networks; Informational security networks; Social, cultural, political, economic and symbolic capitals*

In phase with modern theories that chart the decline of vertical hierarchical social structures and the concomitant rise of horizontal networks (Castells, 1996, 2000; Rhodes, 1997; Friedman, 1999; Wellman, 1999), a number of commentators are reconceptualizing our ways of thinking about policing and security. The seminal report written by Bayley and Shearing (2001) for the National Institute of Justice has, for example, introduced the term "multilateralization" to describe the growing array of auspices and providers—demand and supply—that constitute the modern security assemblage, eschewing the traditional one-dimensional public/private dichotomy. In other texts, Shearing and his colleagues (Shearing & Wood, 2000; Johnston & Shearing, 2003) have developed the concept of "nodal governance" to convey the idea that policing functions and their different organizing modes can now be

Correspondence to: Benoît Dupont, Assistant Professor, School of Criminology, University of Montreal, CP 6128 Succursale Centre-Ville, Montreal QC H3C 3J7, Canada. E-mail: Benoit.Dupont@umontreal.ca. The author is grateful to J.-P. Brodeur, M. Cusson, P. Grabosky, C. Morselli and J. Ratcliffe for their helpful comments on an earlier draft of this article.

ISSN 1043–9463 (print)/ISSN 1477-2728 (online) 
DOI: 10.1080/1043946042000181575

characterized as plural. This line of enquiry is not limited to the authors cited so far, and discrete terminologies notwithstanding, many others have come to similar or related conclusions while examining diverse cultural and geographical contexts (Findlay & Zvekic, 1993; Crawford, 2002; Favarel-Garrigues & Le Huérou in this special issue). Others, while acknowledging the importance of those changes, have questioned to what extent they can be interpreted as a qualitative break with the past, or even as global in reach (Jones & Newburn, 2002a).

According to these authors, the factors at the origins of such profound changes are many and closely interlaced, making it hard, if not impossible, to isolate or to place them in a neat chain of causality. Yet a consensus seems to exist concerning the importance of these factors in explaining the trend toward a more decentralized, horizontal, networked society. The exponential development of information and communication technologies around the globe has, without any doubt, been instrumental in the collapse of all sorts of barriers that previously corseted institutions, organizations, communities and individuals inside limited roles and responsibilities.

Another essential factor has been the effort by the state to rationalize its activities in the wake of the financial crisis experienced in the 1970s, followed by its subsequent divestment from areas that were the symbols of the ubiquitous welfare state. The naval metaphor of a "steering" state that coordinates an army of "rowing" surrogates was quickly embraced as the ideal balance of interventionism and "*laissez-faire*" (Osborne & Gaebler, 1992; Kooiman, 1993).[1] Except in a number of countries where the state jealously retained its strength, no determinism appeared to limit the types of agents involved in the devolution of responsibilities, and private actors became free to cooperate and compete with public entities. This fragmentation, the need for coordination and the uncertainty it created induced the opening of new communication channels between previously isolated players, which in turn contributed to the appearance and reinforcement of partnerships and networks.[2]

In the field of security, the new academic discourses on networks and their governance[3] rest on a set of common premises. First is the realization that the monopoly attributed to the state over the provision of security is more a historical distortion—or at least a temporary anomaly—than a durable condition (Bayley & Shearing, 2001; Johnston, 1992). Even if the distribution of legitimate coercive powers and responsibilities remains a function largely vested in the state (Johnston & Shearing, 2003), private and hybrid organizations now command a growing share of what has become a market, and continuously explore new opportunities. A second tenet of the new discourse on security is that the "public-private" dichotomy that has prevailed until recently fails to account for the diversity and heterogeneity of the actors involved (Brodeur, 1995; Kempa et al., 1999). As the distinction between private and public space fades, as the de-coupling between auspices and providers becomes prevalent, and as security pervades every aspect of modern life, a more complex theoretical framework must be formulated.

Finally, the governance of security is underpinned by a new risk mentality that adds a new layer to the more established punitive mentality (Garland, 1996, 2001; Ericson & Haggerty, 1997; Rose, 2000). This future-oriented rationality is focused on

the prevention and reduction of risk through the intensive use of statistical techniques. In order to appraise risk properly, information must be gathered and exchanged intensively between those that experience it and those who can prevent it and insure against it. The prevalence and multidimensional implications of risk prevent any single player, no matter how large and resourceful, to shoulder it alone. Thus, the creation of partnerships and networks ensure a pooling of resources and a dilution of liability, making risk easier and more acceptable to handle.

However, if the explanatory value of concepts derived from network theories and applied to the security field is indubitable, their use raises almost as many questions as they provide answers. So far, very few empirical studies have been conducted to validate this model and informed intuition remains our best informant. Another question that must be addressed is the tangible dimension of so-called "security networks". The term is in itself vague enough to designate groupings that vary enormously in nature and scale. Despite our fragmented and partial understanding of the processes that shape the reconfiguration of policing and security, we can nonetheless risk a few suggestions that are likely to clarify the use of network terminology in this area of social enquiry. I will also focus on the internal dynamics that define the parameters (position and ties) characterizing agents within a security network, as well as show how particular agents may deploy various forms of resources to develop or maximize their leverage within, or in some cases over, the varied networks to which they belong. First, however, a more systematic approach to security networks is warranted.

## The Small World of Security Networks

So far, I have used the term "security network" indiscriminately, without defining it and without specifying what organizational configurations concretely qualify as a security network. It is now time to be more specific. By "security network", I mean a set of institutional, organizational, communal or individual agents or nodes (Shearing & Wood, 2000) that are interconnected in order to authorize and/or provide security to the benefit of internal or external stakeholders. As Castells (2000: 11) noted, networks are not structurally homogenous; they are made of institutions and internal segmentations of institutions. Structural networks are distinctive of interpersonal networks, an aspect of social life that has been the object of extensive research in the fields of sociology, geography, political science and anthropology (Stinchcombe, 1989). The agents that form them use networks to distribute responsibilities, resources and uncertainty more evenly among themselves, with an effectiveness and efficiency that cannot be matched by vertical command-and-control structures (Kempa et al., 1999). The density of security networks varies greatly from one setting to another, and only certain nodes can fully exploit the opportunities this new form of governance yields. Furthermore, some environments, either for lack of economic attractiveness (no solvent market for private enterprise) or political culture (authoritarian regimes), are not conducive to the emergence of security networks and instead cement the domination of hierarchical structures.

In the field of security, as in every other area of social organization, networks overlap and intersect on a number of levels. Security networks are porous and tracing boundaries can be a perilous exercize. Some are complementary or simply co-exist, while others enter into direct competition. Nor is membership mutually exclusive. This will be determined to a large extent by the size and the jurisdiction of the organization in question: national centralized police services are likely to be connected to more networks than small local agencies. Networks of course differ greatly in mandate, size and scope, but they also have different ways to interact with time and space. All these features will determine, among other things, which actors are included and which are kept out of the network or disconnected.

The burgeoning literature on security networks usually identifies four ideal-types of security networks: local security networks, institutional security networks, international security networks and virtual security networks. Of course, none of the existing security networks actually corresponds exactly to one of the four ideal-types, and there are infinite possible variations, but one feature will tend to dominate the three other dimensions.

### *Local Security Networks*

Local security networks can be defined as initiatives that seek to harness the public and private resources available in local communities in order to overcome complex crime problems that find their origins in deteriorating social conditions. The exponential growth of mega-metropolises and their sprawling populations[4] also call for networked policing, local units being unable to cope with the challenges created by the scale of such urban monsters. Local security networks are tacit acknowledgements by the state of the limitations and ineffectiveness of its fragmented and monopolistic intervention strategies. The nodes in local security networks comprise traditional social control agencies such as the police, local magistrates and social services, but also residential communities, communities of interest, elected officials, business interests, private security providers, and so on (Bayley & Shearing, 2001; Newburn, 2001). Local security networks act as information exchanges on local crime problems and on the resources that can be mobilized to solve them. They rely on local knowledge and solutions that transcend institutional boundaries. In the United Kingdom and France, for example, these networks have been imposed by laws or firmly encouraged by the state (Crawford, 1997; Roché, 2002). In weak states, where government agencies are helpless and not as much part of the solution as part of the problem, the development of local security networks has flowed out from local grassroots initiatives (Dupont et al., n.d.). Local security networks have usually been presented as being polarized around the public-private dichotomy (Johnston, 1992), but the French situation shows that the public can retain centre-stage, and that in such places, the restructuring of security is more aptly understood in terms of a centralized-localized dualism (see Ferret in this special issue).

### *Institutional Networks*

The second category of security network can be located at the institutional level. All security networks involve, of course, institutional nodes to some degree. However, when the explicit purpose of a network is the facilitation of inter-institutional bureaucratic projects or the pooling of resources across government agencies, such a network can be characterized as institutional. Institutional networks differ from local security networks in that they rarely involve community groups or actors outside governmental spheres. They are efficiency-based, where local security networks are more focused on effectiveness. By this I mean that institutional security networks are engaged in an effort to rationalize resources, optimize performance (individual and collective) and maximize the outputs of their members. In the current environment of administrative reform, the flexibility and adaptive capacities of networks constitute very attractive assets and largely explain why they have become so omnipresent. The inward-looking feature of this approach produces relatively closed networks, while local security networks rely on the capacity to connect a much more diverse set of actors, and must retain the ability to integrate new agents at all times in order to produce the expected outcomes. Such networks are primarily found in decentralized policing systems, where local organizations lack the resources to establish and maintain costly structures such as specialized training programmes, forensic capabilities, anti-terrorist resources, research and development centres, and so forth.

An example of an institutional security network constituted over the course of the past 20 years can be found in Australia, where seven state police services and the Australian Federal Police have collaborated to establish common police services at the national level, and administer them on a collective basis under the umbrella of the Australasian Police Minister's Council (Dupont, 2002). These services act as repositories of resources and information that each member of the network can access for a fraction of the price. They also facilitate the transfer and diffusion of innovative practices from one state police force to another. Another example is provided by France, where the size of the national police force and *Gendarmerie* make them fairly self-sufficient, but issue-specific institutional networks have nevertheless been established to deal with terrorism or organized crime, which overcome unproductive competitive approaches. In both of these cases, most of the nodes pre-existed the network but were not linked; where linking did exist, it was limited and sporadic. The networking that occurred was the result of existing agents combining their efforts to design new nodes that would (or so they hoped) facilitate the circulation and sharing of resources.

### *Networks without Borders*

International security networks find their origins in equivalent processes. They share many features with institutional networks, but they must nevertheless be examined separately from them, essentially due to the question of sovereignty. It has been a

common observation among academics who have studied them that international security networks call into question the notion of state sovereignty (Bigo, 1996; Deflem, 2002; Sheptycki, 2002). Administrative structures that support the operations of those networks usually precede their legal sanctioning and supervision by political authorities (Deflem, 2002). It would be excessive to interpret this tendency as reflective of malign intents or through the lens of conspiracy theories. It is more likely the product of the relative bureaucratic autonomy enjoyed by large and complex organizations such as national or federal police services, or international organizations (Norman, 2001) that share a common discourse and "mythologies" on transnational organized crime.

Until recently, these networks were constituted exclusively of state actors from the justice, policing and intelligence areas, but, as in many other facets of the governance of security, non-state players have entered the arena and are seeking increased interactions with these networks. Increasingly, large private security firms operate at the international level, marketing their services to multinational corporations, non-governmental organizations and governments (Johnston, 2000; Dinnen, 2001). They sell expertise and technologies previously restricted to state-security spheres, and often entertain a symbiotic relationship with governments. Some of them receive public funds to manage and deliver police assistance programmes abroad—for example, the contracts won by the American firm Dyncorp include the protection of Afghanistan's President Mohamed Karzai (Baum, 2003), the International Narcotics and Law Enforcement Program and the administration of the International Police Program[5] on behalf of the United States Department of State (Office of Inspector General, 2000; Bureau for International Narcotics and Law Enforcement Affairs, 2003). The British Government is also examining the possibility of subcontracting certain security functions to such companies, providing an acceptable regulatory framework is established first (Foreign and Commonwealth Office, 2002). In other countries such as Australia, government aid agencies regularly outsource police assistance programmes to private or para-public consulting firms.[6] It is still too early, though, to rule conclusively on the importance these private nodes will assume in international security networks, partly because these tend to be characterized by their highly restricted membership.

The structure of international security networks is usually restricted to a single public actor per country involved. This node, which can be a federal, national or specialist unit in the case of single-issue networks, then plays the role of a hub or switch that centralizes all outgoing flows from national sub-units and despatches back all incoming flows. This monopoly over access to the international network's resources and information can result in the disconnection of other national actors from useful resources in countries that have more than one contender for the position of national node (Alain, 2001; Sheptycki, 2002).

### *Informational Networks: Transcending Space and Time*

Finally, instrumental in the emergence of international security networks are virtual

or informational security networks—the technical arrangements allowing the controlled flow of information between security nodes. Virtual networks have accompanied the micro-electronics revolution and created the ability to access instantly information not previously so easily available. Police officers in patrol cars can now request intelligence reports, consult them and update their content while driving from one incident to another. Detectives in one country can access the Interpol restricted-access website in order to consult the notice of a criminal originating from a different country, or its general website for stolen works and confirm the identification of a recovered artefact (Interpol, 2001). The new relation to time and space created by information technologies impacts directly on the creation of security networks that can dilate and collapse traditional spatio-temporal boundaries. Just like the continuous activities of stock markets around the planet, the exchange of police information takes place around the clock in a routine manner, engaging police officers in different time zones in an uninterrupted dialogue that grows louder as new joint databases and telecommunications systems are added.

However, the accelerated pace of technological change challenges the effectiveness of those networks and threatens them with obsolescence almost as soon as they become operational (Marx & Corbett, 1991; Dupont, 2001). The multiplicity of standards and technologies used also limits the connectedness of virtual networks, and leads to the fragmentation and duplication of information. To overcome this difficulty, governments in the post-September 11 environment are investing heavily in the development of technologies that will tighten the existing connections, fill the structural holes and exploit more intensively the information stored in various nodes. The Total Information Awareness programme (renamed "Terrorist Information Awareness" in order to appease wary civil libertarians—see DARPA, 2003), or recent legislative initiatives in the United States, the United Kingdom, France and other countries (Statewatch Observatory, 2003) to enlist the resources of other informational networks in the areas of health, education, travel or leisure, provide examples of attempts to expand the reach of virtual security networks.

Access to these virtual networks, far from being restricted to institutional agents, also extends to private actors and civil society, albeit in a sanitized manner. In North America, a number of police departments are making publicly available through the Internet registers of convicted sexual offenders, maps showing the spatial distribution of crimes (Ratcliffe, 2002) and details of ongoing child abductions with the assistance of media networks.[7] Information exchanges also occur on a systematic level between police services and a range of private and semi-public agencies (Marx, 1987; Ericson & Haggerty, 1997). American law enforcement agencies have, for example, recently gained unrestricted access to the database of European airlines (Amadeus) and can extract 40 different pieces of information on each passenger (Statewatch, 2003). Nonetheless, the conditions leading to the effectiveness of virtual networks are still relatively unclear and results are mixed, as the few intra-organizational empirical studies on the subject have shown (Manning, 2001; Chan et al., 2001).

*The Dilemmas of Security Networks*

The above typology of security networks remains incomplete and based on fragments of information, requiring more empirical and systematic investigations that should focus on features like differentiation or integration of interests and resources, stability, exclusiveness and specialization (Rhodes & Marsh, 1992). It is nevertheless sufficiently detailed to highlight a crucial issue. Notwithstanding the fact that it would be exaggerated to consider all security assemblages involving more than two actors to be a network, we must answer the following question: Should the use of security networks be mainly descriptive in order to better understand the shifts that the policing function is undergoing or should we subscribe to a more normative approach, where security networks are promoted as the new form of security governance? Johnston and Shearing (2003) argue that security networks (or "nodal governance" to use their own term) provide more opportunities for transforming existing relations "in ways that could advance just and democratic outcomes", but they also concede that power inequalities subsist and that the right conditions must be met. It would seem, then, that a normative approach to security networks holds considerable benefits in terms of adjusting security authorization and provision to a broad range of contexts, but that the complexity of required conditions currently limits our capacity to engineer nodal governance.

There is, for example, no doubt that traditional accountability and evaluation mechanisms are not adapted to the morphology of security networks. Existing regulatory means are usually focused on the actions of single organizations or individuals operating in well-defined sectors or domains, but do not appear to be properly equipped to deal with coalitions of interests transcending these boundaries (Perrucci & Potter, 1989). In recent efforts by American law enforcement agencies to eradicate terrorism, we can witness the deliberate recourse to network strategies in order to circumvent legal-hierarchical controls designed to prevent the use of torture (The Economist, 2003). Attempts to design network-centric regulatory entities, such as the Patten Commission's recommendation to create a *policing* board instead of a *police* board (Shearing, 2000), are still isolated occurrences. Chan (1999) has charted the meta-accountability mechanisms that envelop modern police organizations, and Stenning (2000) has explored the hidden facets of private security accountability, but in both cases, the authors uncover multiple, fragmented and unconnected layers of accountability. The reflective accountability mechanisms needed in the security networks era are still in their infancy (Loader, 2000), and many other areas of state intervention face the same dilemma (Tshuma, 2000; Considine, 2002).

In the area of effectiveness, performance evaluation tools still rarely penetrate the dynamics of networks (Johnston, 1998). How security networks affect individual and aggregated organizational performance, and what they can achieve in terms of results, has only attracted scant attention so far. This can be attributed partly to the pervasion of a hierarchical vertical mentality among evaluators, but also to the inherent complexity of what Stinchcombe (1989) calls "conditional network effects":

some networks have larger effects under some conditions than others, and assessing those effects and causal relations under such premises is relatively complicated.

These obstacles are compounded by the fact that the structural conditions of networks are mediated by a complex set of interactions linking the nodes together. The internal and external dynamics of networks are primarily determined by a contest among actors for dominant or central positions in order to maximize the benefits and minimize the risks associated with their participation. Networks are not egalitarian social structures, and some members are quite powerful while others are barely capable of maintaining their connections. These simultaneous relations of power and cooperation determine the existence and functioning of security networks as much as external circumstances and constraints.

Of course, the views and attitudes of individuals in charge of implementing network-centered policies greatly influence the outcomes of such strategies. Crawford (1994) has, for example, highlighted the shared anxieties and ideological dissonance that can impact negatively on inter-agency cooperation. The role of interpersonal relationships in security networks is paramount, mainly because of its informal capacity to structure them. However, my main concern in this article lies at the structural level. In order to represent the strategies used by network nodes to maintain or improve their position, I will use the "capital" metaphor.

## Nodes, Positions and Capitals: The Dynamics of Networks

If networks are infused with collaborative values, they can also be construed at the sub-network level as spaces of conflict or competition opposing the various nodes that compose them. The stakes of these conflicts are the maximization of resources extracted from the network, taking into account the resources contributed.

### *Within-network Strategies*

Agents will mobilize different types of "capital"—or context-specific resources—already in their possession in order to influence the operating parameters of the network and achieve their desired outcome. Additionally, they will also frame the appropriation or the redefinition processes associated with capitals specific to the network in question. By doing so, they seek to monopolize capitals that are recognized as legitimate by all members of the network and delimit the parameters of the consensus holding the network together.

These capitals are unequally distributed among the organizations and individuals forming the network, meaning that there are dominant and dominated actors. It must be unequivocally stated that capital should not only be envisaged as an economic asset; it can take various forms that can be as (or even more) valuable in a given network than money. This unequal distribution of capital determines to a significant degree the structure of the network, which is shaped by the temporary outcome of a historical contest between the forces composing the network. Because of the dual positions encountered within networks (dominant-dominated), the

strategies deployed by the nodes tend to adopt a similar binary classification: strategies of stability and conservation revolving around the capitals progressively accumulated are favoured by the established "orthodox" actors, while new nodes (heterodox actors) seek to alter the existing order through innovative and subversive strategies. Thus, in the case of local security networks, where private providers are introducing new practices and mentalities, police agencies will emphasize the three legitimate dominant capitals (political, cultural and symbolic) as opposed to reliance on economic and social capitals by private and hybrid agents. Of course, this conflict must be relativized: since all actors have invested heavily to enter the network, they have a vested interest in its preservation, hence sharing an "objective complicity" that transcends their divergence. Finally, it must be stated that external factors weigh heavily on internal struggles and can even destabilize networks. However, collective actors rapidly integrate these new environmental constraints, and the inherent flexibility of the nodal structure allows networks to demonstrate a surprising resilience (Bourdieu, 1984; Lahire, 2001).

### *Cultural, Social, Political, Economic and Symbolic Capitals as Strategic Assets*

Five different forms of capital (Alain, 2002; Dupont, 2003) can be highlighted as being relevant in the context of security networks. I will list and define those five capitals, while at the same time showing how they are generally used as strategic assets to acquire or maintain a dominant position within security networks. *Economic capital* refers to the traditional meaning of financial resources allocated through the fiscal process or the "invisible hand" of the market. Private providers, contrary to their public counterparts, do not face the dilemmas of budget cuts and are free to pursue aggressively new profitable opportunities. While the accumulation of economic capital is an end in itself for private providers, public actors will tend to see it as a currency to be converted into more legitimate forms of capital such as cultural, political and symbolic capital. In countries where policing functions are distributed across a number of jurisdictions and competing institutions, economic capital will also dictate the patterns found in security networks.

*Political capital* derives from the proximity of actors to the machinery of government and their capacity to influence or direct this machinery toward their own objectives. As agencies central to the manifestation of the sovereignty of the state (Garland, 1996), police organizations have amassed a considerable amount of political capital that is, for example, mediated through police-politician relations, law and order rhetorical auctions regularly held during elections, or the vocal campaigns of police unions. By comparison, private security companies are relatively poor in political capital. Of course, there are temporal and structural variations in the quantity of political capital at the disposal of organizations. Those operating in a decentralized and/or fragmented system will have to share their political capital with other actors, while a centralized unified police will be in a better position to concentrate political capital (Bayley, 1985).

The third form of capital is *cultural capital*. The professionalization of policing has

been accompanied by the creation of a unique expertise in the field of crime prevention and detection, which is accumulated and transmitted through higher levels of selection and training, the development of research and development programmes, and the incessant adoption and upgrade of new crime control technologies. This aggregate of knowledge and expertise constitutes cultural capital. The emphasis on cultural capital found in police organizations, particularly among specialist units, cannot be matched by private security companies, although the market is increasingly offering services that were previously the preserve of government agencies, eroding the superiority of the police in the area of cultural capital. Members that are able to mobilize vast amounts of expertise will be in a better position to leverage the network's resources, or will be relied upon to lead the coordination efforts.

*Social capital*, the fourth form of capital—defined as the whole set of social relations that allow the constitution, maintenance and expansion of social networks—has long been associated with opportunities for political interference and corruption in the field of security. This justified a period of professionalization and bureaucratization for the police to the detriment of the informal mechanisms of social control that linked the police and the public. Private security providers and non-governmental organizations, on the contrary, can rely on much larger reserves of social capital and will use this as a negotiating tool to manoeuvre inside networks.

Finally, the four previous forms or capital are mediated through *symbolic capital*, which is the most general form of capital. It refers to the mechanisms that confer legitimacy to an organization, and the power it holds to speak with authority to the other actors. In the field of security, the current allocation of symbolic capital allows the public police to question the legitimacy of non-governmental actors. However, the distribution of symbolic capital has not always been to the benefit of the police, particularly in the early days of the institution, when a strong opposition elicited concessions from the proponents of a professional uniformed police (Reiner, 1992; Storch, 1975). However, as political and cultural capitals were slowly accumulated and transmitted, symbolic capital materialized and strengthened the position of the police, starting a loop whereby it became instrumental in procuring more political, cultural and economic resources. However, this historical trend seems to have reached a peak. Recent failures of the police to control crime and its everyday manifestations have provoked erosion of the symbolic capital it holds. In this context, too much symbolic capital can become a liability and create a window of opportunity for new actors.

The diversity of capitals mobilized by security nodes barely reflects the diversity of interests, objectives and resources found in inter-organizational networks, but it can help us understand the intrinsic complexity of intra-network interactions. Additionally, it also constitutes a warning against the temptation to portray networks as static mechanistic structures. Instead, it attempts to analyze the latent competition occurring between nodes to dominate the network through the deployment of the five forms of capital enumerated above. I emphasized in the illustrations of how political,

cultural, social, economic and symbolic capitals are accumulated and "invested" the differences that distinguish public nodes from their private counterparts. These variations in the distribution of capitals and their impact on the anatomy of security networks are not restricted to "multilateralized" contexts, and strong states, where the privatization of security has not reached the same levels, are also the scene of huge disparities among governmental actors. In this particular configuration, the central-local polarization defines the capital-allocation formula and the resulting position in security networks (see Ferret and Ocqueteau in this special issue). The recourse to the capital metaphor also allows us to better conceptualize the exchanges taking place between actors and network nodes, some capitals being traded, purchased, discarded, assigned to, or demanded from others (Grabosky, 2002).

## Conclusion

In this article, I have assumed, on the basis of a first cut of influential works, that networks are increasingly becoming a key element in the governance of security. I have also tried to develop the concept of "security network" and raise some criticisms at the level of theory, highlighting variations in scope, structures, mentalities and technologies. This account does not pretend that the transformations undergone in the field of security are identical in all countries. Instead, it offers a conceptual interpretation in phase with the changes encountered in other political, economic and social realms on a global scale. To be sure, country variations persist. For example, if Anglo-Saxon scholars seem to agree on the pluralization of policing, implying a more intensive involvement on the part of private providers, Continental observers of the police, and especially French scholars, are resisting that line of inquiry. This should remind us that national contexts differ greatly and warn us against a tendency to assign a global significance to developments occurring in the United States, Canada or the United Kingdom. Continental Europe, Africa, Latin America and Asia might follow different paths that need to be understood as well as the trends described above.

However, one theme that unites those views of modern policing in late modern societies is the diffusion of responsibilities, either inside or outside government, through the generalization of network structures (Jouve, 1995). Hence, the security network approach offers a common conceptual platform to interpret the complexification of security provision across a whole spectrum of configurations and can bridge the gap between state-centric and pluralist views of security (others refer to hierarchy and market, see, e.g., Powell, 1990). Its relevance is augmented by the fact that networks, whether they are coordinated by the state or more plural in form, are linked to each other at one level or another and, as a result, operate inter-network transfers that impact significantly on the governance of security (Jones & Newburn, 2002b). The right question to ask would then not be at what stage of security privatization a country has arrived, implicitly assigning a positive image to pluralistic modes, but instead what is the morphology of security networks operating in certain

societies, and what is their level of interconnection/integration with other networks at the local, national and international levels?

In particular, two sets of empirical questions warrant more detailed investigations. The first one deals with the process of transformation in the field of security, from vertical hierarchical structures to horizontal networks. The formation of security networks and the adaptive strategies deployed by public and private institutions to adjust to nodal governance need to be documented more thoroughly. For example, what is the relative effectiveness of spontaneous versus designed security networks? What is the impact of the sectoral composition of security networks (public, private, various mixes) on outcomes? Do certain types of security networks, such as the ones outlined in the first part of this article, generate particular forms of linkages and power relations (coercive, dominant, parasitic, symbiotic, etc.)? The second set of questions is related to the changes experienced by security networks over time, particularly in terms of membership, leadership and responsiveness to external factors. What drives security networks to expand, to include or exclude nodes? What are the effects of changing conditions on security networks? Do security networks generate new knowledge, as do epistemic communities? I have shown how the capital metaphor can be used to understand the internal dynamics of networks. Of course, it is to be expected that different types of networks will resort to those various capitals following different patterns. Documenting and understanding those patterns, as well as their outcomes on the production and distribution of security, is of great importance if attempts to improve the effectiveness, efficiency and accountability of those new security assemblages are to be made.

## Notes

[1] It is however surprising that no one thus far has risked an analogy with the galleys, where prisoners chained to their bench rowed in cadence, determined by the speed and the direction the captain needed to achieve, with those too exhausted to follow the beat being flogged in the hope that this would boost their stamina. The new "steering and rowing" imagery appears to involve a more consensual form of collaboration.

[2] For a detailed discussion of "the rhetoric and reality of public-private partnerships", see Wettenhall (2003).

[3] For a valuable discussion of the limits of the term "policing" as a semantic tool to explore issues related to social order and security, mainly because of its systematic association with the idea of public police institutions, see Johnston and Shearing (2003: 10).

[4] According to the United Nations Population Division, an urban agglomeration qualifies as a mega-city when it reaches ten million persons. In 1950, there was only one: New York. By 1975, there were five of them, 16 in 2000, and projections estimate that there will be 21 such metropolises by 2015 (United Nations Population Division, 2002: 93).

[5] This programme provides American peace monitors under United Nations supervision in places such as Bosnia, Kosovo and East Timor.

[6] Such companies include ACIL and Overseas Project Corporation of Victoria in Australia.

[7] Known as "Amber alerts", this system relies on thousands of voluntary users who download a screensaver onto their computer. When a child is abducted, the police uses the screensaver to broadcast details of the child and abductor. E-mail, news tickers and other media alerts are also sent out to people living in the area of the abduction (see www.codeamber.org).

## References

Alain, M. (2001), "The trapeze artist and the ground crew: Police cooperation and intelligence exchange mechanisms in Europe and North America: A comparative empirical study", *Policing and Society*, Vol. 11, no. 1, pp. 1–27.

Alain, M. (2002), "Au-delà de la bonne volonté: Enjeux et compétitions dans le champ de la sécurité", Paper prepared for the "In Search of Security" conference, hosted by the Law Commission of Canada, 19–22 February.

Baum, B. (2003), "The Pentagon's private army", *Wired Magazine*, Vol. 11, no. 2, pp. 119–123.

Bayley, D.H. (1985), *Patterns of Policing*, Rutgers University Press, New Brunswick, NJ.

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

Bigo, D. (1996), *Polices en réseaux: L'expérience Européenne*, Presses de Sciences Politique, Paris.

Bourdieu, P. (1984), Quelques propriétés des champs, in: *Questions de sociologie*, Les Éditions de Minuit, Paris.

Brodeur, J.-P. (1995), "Le contrôle social: Privatisation et technocratie", *Déviance et Société*, Vol. 19, no. 2, pp. 127–147.

Bureau for International Narcotics and Law Enforcement Affairs (2003), *The United States and International Civilian Policing (CIVPOL): Fact Sheet*, United States Department of State, Washington, DC.

Castells, M. (1996), *The Information Age: Economy, Society and Culture,* Vol. 1: *The Rise of the Network Society*, Blackwell, Cambridge.

Castells, M. (2000), "Materials for an exploratory theory of the network society", *British Journal of Sociology*, Vol. 51, no. 1, pp. 5–24.

Chan, J.B.L (1999), "Governing police practice: The limits of the new accountability", *British Journal of Sociology*, Vol. 50, no. 2, pp. 251–270.

Chan, J.B.L. et al. (2001), *E-policing: The Impact of Information Technology on Police Practices*, Criminal Justice Commission, Brisbane.

Considine, M. (2002), "The end of the line? Accountable governance in the age of networks, partnerships and joined-up services", *Governance: An International Journal of Policy, Administration and Institutions*, Vol. 15, no. 1, pp. 21–40.

Crawford, A. (1997), *The Local Governance of Crime: Appeals to Community and Partnerships*, Clarendon Press, Oxford.

Crawford, A. (1994), "Social values and managerial goals: Police and probation officers' experiences and views of inter-agency cooperation", *Policing and Society*, Vol. 4, no. 4, pp. 323–339.

Crawford, A. (ed) (2002), *Crime and Insecurity: The Governance of Aafety in Europe*, Willan, Cullompton.

DARPA (2003), *Report to Congress Regarding the Terrorism Information Awareness Program*, United States Department of Defense, Washington, DC.

Deflem, M. (2002), *Policing World Society: Historical Foundations of International Police Cooperation*, Oxford University Press, Oxford.

Dinnen, S. (2001), *Law and Order in a Weak State*, Crawford House, Adelaide.

Dupont, B. (2001), Policing and the information age: Technological errors of the past in perspective, in: Dupont, B. & Enders, M. (eds) *Policing the Lucky Country*, Federation Press, Sydney.

Dupont, B. (2002), *Construction et réforme d'une police: Le cas Australien (1788–2000)*, L'Harmattan, Paris.

Dupont, B. (2003), "Public entrepreneurs in the field of security: An oral history of Australian police commissioners", Paper prepared for the "In Search of Security" conference, hosted by the Law Commission of Canada, Montreal, 19–22 February.

Dupont, B., Grabosky, P. & Shearing, C. (n.d.), The Governance of Security in Weak and Failing States (draft).

Ericson, R.V. & Haggerty, K.D. (1997), *Policing the Risk Society*, University of Toronto Press, Toronto.

Findlay, M. & Zvekic, U. (eds) (1993), *Alternative Policing Styles: Cross-cultural Perspectives*, Kluwer, Deventer.

Foreign and Commonwealth Office (2002), *Private Military Companies: Options for Regulation*, HMSO, London.

Friedman, L.M. (1999), *The Horizontal Society*, Yale University Press, New Haven, CT.

Garland, D. (1996), "The limits of the sovereign state: Strategies of crime control in contemporary society", *British Journal of Criminology*, Vol. 36, no. 4, pp. 445–471.

Garland, D. (2001), *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford University Press, Oxford.

Grabosky, P. (2002), Private sponsorship of public policing. Unpublished paper prepared for the Regulatory Institutions Network Seminar Series, Australian National University, Canberra.

Interpol (2001), *Interpol at Work 2001*, OIPC Interpol, Lyon.

Johnston, L. (1992), *The Rebirth of Private Policing*, Routledge, London.

Johnston, L. (1998), Late modernity, governance and policing, in: Brodeur, J.-P. (ed) *How to Recognise Good Policing: Problems and Issues*, Sage, Thousand Oaks, CA.

Johnston, L. (2000), Transnational private policing: The impact of global commercial security, in: Sheptycki, J. (ed) *Issues in Transnational Policing*, Routledge, London.

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

Jones, T. & Newburn, T. (2002a), "The transformation of policing? Understanding current trends in policing systems", *British Journal of Criminology*, Vol. 42, pp. 129–146.

Jones, T. & Newburn, T. (2002b), "Learning from Uncle Sam? Exploring US influences on British crime control policies", *Governance: An International Journal of Policy, Administration and Institutions*, Vol. 15, no. 1, pp. 97–119.

Jouve, B. (1995), Réseaux et communautés de politique publique en action, in: Le Galès, P. & Thatcher, M. (eds) *Les réseaux de politique publique: Débat autour des policy networks*, L'Harmattan, Paris.

Kempa, M. et al. (1999), "Reflections on the evolving concept of 'private policing'", *European Journal on Criminal Policy and Research*, Vol. 7, pp. 197–223.

Kooiman, J. (ed) (1993), *Modern Governance: New Government–Society Interactions*, Sage, London.

Lahire, B. (2001), Champ, hors-champ, contrechamp, in: *Le travail sociologique de Pierre Bourdieu*, La Découverte, Paris.

Loader, I. (2000), "Plural policing and democratic governance", *Social & Legal Studies*, Vol. 9, no. 3, pp. 323–345.

Manning, P.K. (2001), "Technology's ways: Information technology, crime analysis and the rationalizing of policing", *Criminal Justice*, Vol. 1, no. 1, pp. 83–103.

Marx, G.T. (1987), The interweaving of private and public police in undercover work, in: Shearing, C. & Stenning, P. (eds) *Private Policing*, Sage, Newbury Park, CA.

Marx, G.T. & Corbett, R. (1991), "Critique: No soul in the new machine: Technofallacies in the electronic monitoring movement", *Justice Quarterly*, Vol. 8, no. 3, pp. 399–414.

Newburn, T. (2001), "The commodification of policing: Security networks in the late modern city", *Urban Studies*, Vol. 38, no. 5–6, pp. 829–848.

Norman, P. (2001), Policing "high tech crime" in the global context: The role of transnational policy networks, in: Wall, D. (ed), *Crime and the Internet: Cybercrimes and Cyberfears*, Routledge, London.

Office of Inspector General (2000), *Review of INL-administered Programs in Colombia: Report of Audit*, United States Department of State, Washington, DC.

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

Perrucci, R. & Potter, R. (1989), The collective actor in organizational analysis, in: *Networks of Power: Organizational Actors at the National, Corporate and Community Levels*, Aldine de Gruyter, New York.

Powell, W. (1990), "Neither market nor hierarchy: Network forms of organization", *Research in Organizational Behavior*, Vol. 12, pp. 295–336.

Ratcliffe, J. (2002), "Damned if you don't, damned if you do: Crime mapping and its implications in the real world", *Policing and Society*, Vol. 12, no. 3, pp. 211–225.

Reiner, R. (1992), *The Politics of the Police*, Harvester Wheatsheaf, Hemel Hempstead.

Rhodes, R.A.W. (1997), *Understanding Governance: Policy Networks, Governance, Accountability and Reflexivity*, Open University Press, Buckingham.

Rhodes, R.A.W. & Marsh, R. (1992), Policy networks in British politics, in: Marsh, R. & Rhodes, R.A.W. (eds) *Policy Networks in British Government*, Clarendon Press, Oxford.

Roché S. (2002), Towards a new governance of crime and insecurity in France, in: Crawford, A. (ed) *Crime and Insecurity*, Willan, Cullompton.

Rose, N. (2000), "Government and control", *The British Journal of Criminology*, Vol. 40, no. 2, pp. 321–339.

Shearing, C. (2000), "'A new beginning' for policing", *Journal of Law and Society*, Vol. 27, no. 3, pp. 386–393.

Shearing, C. & Wood, J. (2000), "Reflections on the governance of security: A normative enquiry", *Police Practice*, Vol. 1, no. 4, pp. 457–476.

Sheptycki, J. (2002), *In Search of Transnational Policing*, Ashgate, Avebury.

Statewatch (2003), "EU airlines allowing access to all personal details on passengers by US authorities", *Statewatch News*. Available online at: www.statewatch.org/news/2003/jul/09usdata.htm (accessed 8 July 2003).

Statewatch Observatory (2003), *In Defense of Freedom and Democracy: New Laws and Practices Affecting Civil Liberties and Rights after 11 September 2001*. Available online at: www.statewatch.org/observatory2.htm (accessed 21 July 2003).

Stenning, P. (2000), "Powers and accountability of the private police", *European Journal on Criminal Policy and Research*, Vol. 8, no. 3, pp. 325–352.

Stinchcombe, A. (1989), An outsider's view of network analyses of power. in: Petrucci, R. & Potter, H. (eds) *Networks of Power*, Aldine de Gruyter, New York.

Storch, R. (1975), "The plague of the blue locusts: Police reform and popular resistance in Northern England, 1840–1857", *International Review of Social History*, Vol. 20, pp. 61–90.

The Economist (2003), "Ends, means and barbarity", *The Economist*, Vol. 366, no. 8306, pp. 18–20.

Tshuma, L. (2000), "Hierarchies and government versus networks and governance: Competing regulatory paradigms in global economic regulation", *Social & Legal Studies*, Vol. 9, no. 1, pp. 115–142.

United Nations Population Division (2002), *World Urbanization Prospects: The 2001 Revision*, United Nations Publications, New York.

Wellman, B. (ed) (1999), *Networks in the Global Village*, Westview Press, Boulder, CO.

Wettenhall, R. (2003), "The rhetoric and reality or public-private partnerships", *Public Organization Review: A Global Journal*, Vol. 3, pp. 77–107.

*Received 3 August 2003*
*Revised 8 September 2003*
*Accepted 7 October 2003*