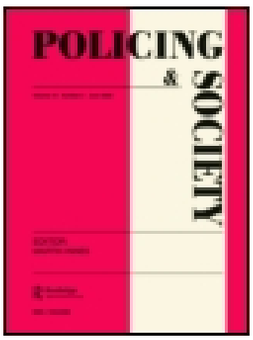

Routledge
Taylor & Francis Group

Policing and Society

An International Journal of Research and Policy

ISSN: 1043-9463 (Print) 1477-2728 (Online) Journal homepage: http://www.tandfonline.com/loi/gpas20

Taking stock of networks across the security field: a review, typology and research agenda

Chad Whelan & Benoît Dupont

To cite this article: Chad Whelan & Benoît Dupont (2017): Taking stock of networks across the security field: a review, typology and research agenda, Policing and Society, DOI: 10.1080/10439463.2017.1356297

To link to this article: http://dx.doi.org/10.1080/10439463.2017.1356297

POLICING AND SOCIETY, 2017
https://doi.org/10.1080/10439463.2017.1356297

Taking stock of networks across the security field: a review, typology and research agenda

Chad Whelan[a] and Benoît Dupont[b]

[a]Department of Criminology, School of Humanities and Social Sciences, Deakin University, Geelong, Australia; [b]International Centre for Comparative Criminology, Université de Montréal, Montreal, Canada

ABSTRACT

Security network research has grown considerably in the last decade as it has been increasingly recognised that security is pursued through networks of public, private and hybrid actors or nodes. This research deals with local, institutional, international and virtual security networks and includes techniques such as social network analysis and approaches more familiar to organisational theory and management. However, much of the security network research employs the network concept as a metaphor to suggest a relationship between a set of security nodes, without examining the structural pattern of these relationships or the underlying properties of security networks. Different uses of the network concept have led to confusion about the application of network theory across the security field. This article attempts to address these issues by clarifying the fundamental concepts of a network perspective and revisiting existing typologies of security networks. We review research on the use of network perspectives across the security field, evaluate theoretical and empirical trends, and give directions for future research. We examine the geographical properties of security networks operating at the subnational, national and transnational levels and put forward four types of networks that have the potential to improve security network research: information exchange networks, knowledge generating networks, problem-solving networks and coordination networks. The article concludes by highlighting the importance of networks for understanding and promoting the governance of security.

ARTICLE HISTORY
Received 8 February 2017
Accepted 12 July 2017

KEYWORDS
Security networks; security governance; security; policing; police partnerships; networks

Introduction

Security is increasingly recognised as being pursued through networks of public, private and hybrid actors or nodes. Following the 'nodal governance' perspective (Johnston and Shearing 2003, Wood and Dupont 2006), scholars have emphasised how mentalities and technologies of security governance have evolved from a more state-centered approach to one involving an array of potential governing nodes. Grabosky (1995) was among the first to highlight the diverse range of mechanisms that can be used to enlist non-governmental commercial and voluntary institutions in the co-production of regulatory compliance. While these regulatory or security nodes may or may not form ties or enter networks, and while the precise nature of these ties is not always the direct focus of advocates of nodal governance, it is important to distinguish between the nodal governance and security network perspectives. The main focus of the nodal governance perspective has been to argue that no particular node – such as the state – should be given priority in networks of security governance. It is perhaps this particular point that attracted most attention, with scholars adopting a normative

CONTACT Chad Whelan chad.whelan@deakin.edu.au

position with regard to the central role of the state in such networks (Loader and Walker 2007). Following a related but at times quite different trajectory, research on security networks and related themes such as partnerships has grown considerably in the last decade. This body of research extends to what one of us calls local, institutional, international and virtual security networks (Dupont 2004) across the field of 'low' to 'high' policing (Brodeur 2010). Security network research now encompasses researchers using techniques such as social network analysis (SNA) (Dupont 2006, Brewer 2014) as well as those calling attention to the organisational dynamics of networked forms of security governance (Whelan 2012). Security network research differs from nodal governance in that it is more focused on *networks* rather than *governance*. It is, as such, less concerned with the attributes of individual security nodes than it is the relationship between a given set of nodes and the underlying properties of such relationships.

By expanding its focus of enquiry to capture the diversity of institutions, capacities, linkages and interactions contributing to defining and responding to particular security problems, security network research overcomes one of the major limitations experienced by police scholars attempting to analyse the contribution of police organisations to the delivery of security. That is, they find it exceedingly difficult to accurately assess the impact of a single institution on complex crime and security problems, no matter how powerful that institution proves to be. Some private security scholars who legitimately raise the instrumental features and democratic shortcomings of this specific mode of security delivery face a similar challenge; reducing the contribution of private security providers to commodified exchanges fails to account for the complex web of formal and informal relationships and constraints that shape their operations (Dupont 2014). The security network approach frames security as the cumulative outcome of activities undertaken by a broad and diverse range of interdependent institutions. For example, in the field of counter-terrorism, security network research seeks to move beyond analysing how security agencies address the terrorist threat, evaluating policy or legislation, or focusing on the organisational failures that may have preceded a particular attack. Instead, it focuses on 'structural' properties such as how institutional networks form and adapt in response to perceived threats and what governance mechanisms emerge as a result, and 'relational' dynamics such as how organisational cultures and interpersonal relationships enable and constrain these arrangements (Whelan 2012). The broader scope of this approach makes it more challenging, both theoretically and empirically, but also potentially more rewarding. In light of the considerable growth in network research and diverse methodological approaches, it is time to take stock of the security network literature in the form of a systematic review that provides directions for future research.

This article aims to clarify the fundamental concepts associated with a network perspective and assess the current state of empirical knowledge on security networks. We argue that current security network research has many limitations. For example, different uses of the concept of network have generated confusion about how network theory should be applied across the security field. A large volume of research employs the network concept as a metaphor to suggest a relationship between a set of security nodes but fails to examine the structural pattern of these relationships or the organisational properties of security networks. Much of the literature focuses on partnerships, which we take to include dyads (two actors), whereas our definition of network, commensurate with leading approaches in organisational (Kilduff and Tsai 2003) and public administration research (Provan and Kenis 2008), is based on groups (three or more actors). We suggest that the network concept only ceases to be employed as a metaphor when researchers focus on actual security networks and can identify their structural and relational properties, which requires researchers to adopt an analytical or organisational network perspective. We therefore argue that in order to advance security network research, we need to develop our language and tools with which to analyse and understand security networks.

The article is organised in three sections. First, we outline the context and method of our systematic review of the security network literature, which uses two main categories: network terminology and network form. Our objective is to highlight the different ways in which security networks have

been studied and to call for greater consistency in these approaches, particularly by drawing on leading network research in other disciplines. The second section uses our assessment of the security network literature to revisit Dupont's (2004) typology of security networks. We review the geographical and functional features of this typology to provide guidance for further research on specific types of security networks, their unique properties and dynamics. Drawing on the inter-organisational network literature (Popp *et al.* 2014), we call attention to four types of networks that we believe have much relevance across the security field: information exchange networks, knowledge generating networks, problem-solving networks and coordination networks. We present these ideal-types as a heuristic device with which to develop the language of security network research. In particular, we hope that these network types will assist future research move beyond the metaphorical use of the network concept by bringing into focus certain features of different networks. Third, we map out a research agenda that addresses our requirements for more consistent network terminology and approaches as well as specific gaps in knowledge. We focus on both the methodological approaches used to study networks and the types of security networks that have been studied. Due to space constraints, we will not address the specific algorithms and mathematical techniques that can be used to study networks (Borgatti *et al.* 2013). The article concludes by highlighting the importance of furthering our knowledge of networks in order to better understand the governance of security.

A systematic review of the security networks literature

Context and methods

The network mode of organisation, with its promises of a less hierarchical, more empowered, innovative and productive world, has captured the imagination of social theorists, who conceptualised it as the natural by-product of the rise of technical and computer networks (Powell 1990, Castells 1996, 2000, Jones *et al.* 1997, Castells and Cardoso 2005, Latour 2005, Benkler 2006, Rainie and Wellman 2012). In the criminology and policing literature, this larger narrative is reflected in the growing realisation that the myth of the state's hegemonic control over the authorisation and delivery of security should be replaced by acknowledgment of more diffuse arrangements involving a broad range of private and hybrid organisations undertaking policing functions (Jones and Newburn 1998, 2006, Loader 1999, Bayley and Shearing 2001, Johnston and Shearing 2003, Wood and Dupont 2006, Ayling *et al.* 2009, Brodeur 2010, Schuilenburg 2015). Although the network terminology had occasionally been used to describe these expanding security arrangements, discussions remained largely metaphorical until the publication of Dupont's (2004) programmatic paper in *Policing and Society*.

That article, which took note of the recent advances made by social network analysts to understand complex social phenomena (Wasserman and Galaskiewicz 1994, Watts 2003), defined security networks as 'a set of institutional, organisational, communal or individual agents or nodes that are interconnected in order to authorise and/or provide security to the benefit of internal or external stakeholders' (Dupont 2004, p. 78) and then provided a typology of existing security networks (local, institutional, international, informational). Dupont leverages Bourdieu's (1986) seminal notion of five forms of capital to illuminate how security nodes navigate complex sets of relationships to achieve desired individual and collective outcomes. He then calls for the development of a 'common conceptual platform to interpret the complexification of security provision across a whole spectrum of configurations' that could bridge the gap between state-centric and pluralist views of security (Dupont 2004, p. 87). The article argues that two areas of empirical research should be prioritised: generating a pool of case studies that examine the core features of security networks in a broad range of national and local contexts; and assessing the dynamic impact of these configurations on security outcomes. Using the analytical tools usually applied to 'dark' networks (Raab and Milward 2003) – a term that refers to both illicit and covert networks that depend heavily on trust relations to maintain their cohesion but also rely heavily on coercion and physical force for management and conflict resolution – a growing number of policing scholars started to explore security as an interactive process involving a complex web of institutional actors.

The security network approach has, however, always been more a diffuse sensibility than a hard paradigm. Rather than drawing from a single source of inspiration, Dupont's (2004) article reflected shifting social science and public policy landscapes that facilitated a match between a complex problem (fragmenting security) and new theoretical and methodological tools. More than 10 years after its publication, it seems relevant to assess the literature on security networks and its contribution to our understanding of contemporary policing. In particular, we believe it is important to look at what types of security networks have been studied, whether a consistent terminology been employed, what methods have been used, what types of data have been collected, and which research gaps and opportunities should become the focus of our attention.

To answer these questions as systematically as possible, we conducted an extensive search of three major bibliographic databases (criminal justice abstracts, sociological abstracts and social sciences full text) for articles published in the last 12 years that used the terms 'policing' and/or 'security', 'networks' and/or 'partnerships' or variations in journal titles, abstracts or key words. Our initial search, conducted during the second half of 2015, found over 500 academic articles, which we then categorised manually. First, we excluded articles that focused exclusively on dark networks as well as those that dealt with networks only superficially. A more difficult – and not entirely satisfactory – decision was to set aside a large proportion of the works on partnerships because, although some large partnerships operate as networks and are studied as such, most research on the subject emphasises the nature and quality of bilateral ties (or dyads). We considered only contributions focusing on groups (three or more actors). We also included only a limited number of contributions from the third-party policing literature. This strategy focuses on a vast network of guardian institutions that can be coerced by the police to prevent disorder (Buerger and Green Mazerolle 1998). Even when a more cooperative view of third-party policing is outlined (Mazerolle and Ransley 2006), the analysis is often primarily concerned with the police role and effectiveness in instrumentalising potential partners, laws and regulations and less interested in the underlying structure and dynamics of the third-party policing network as a whole.

We ended up with 117 journal articles, books and book chapters that form the basis of this review. Articles were then coded using a template that extracted relevant details across eighteen categories listed in Table 1, which include definition, type and size of network under analysis, geographical scope, security issues addressed, nature of ties, performance assessment and accountability. We concentrate on three key aspects: network terminology, methodological approaches and the forms of networks under analysis. In each of these categories we find considerable disparities among researchers, suggesting that a shared approach would offer significant benefits for security network research.

Table 1. List of categories used to code the 117 articles in our sample.

Category	Subcategory
Source information	Author(s)
	Date of publication (range: 2004–2015)
	Title
Definition used	Focus: network (56%); partnership (26%); other (18%)
	Full text of definition extracted (53 definitions)
Theoretical framework	Prominent author(s) cited
	Focus on network as goal-directed (35%); emergent (23%); metaphor (37%); other (5%)
Methodology	Source(s) of data
	Number of network nodes analysed (range: 3–103)
	Type of analysis: quantitative (4%); qualitative (79%); mixed methods (16%)
Geography	Country location (24 different countries)
	Scope: subnational 61%; national (21%); international (14%); various (4%)
Institutional sectors	Nodes: public (19%); private (0%); hybrid (81%)
Security issues	General policing/urban security/terrorism/transport security/cyber-crime/etc. (see Table 2 for details)
Nature of ties	Informal (6%); formal (7%); both (87%)
Assessment	Effectiveness of security networks (2 studies attempted to quantitatively measure network effectiveness or impact)
	Accountability mechanisms
	Recommendations for future studies

Network terminology: defining networks, nodes and ties

Networks consist of nodes and ties. Nodes, or actors, can represent individuals, groups, organisations, or any other entity. Ties, or relationships, are what connect the nodes. These ties can indicate communication between nodes, such as advice and information exchange, but they can also reflect more substantive transactions, such as resource pooling. Relationships may be either formal, based on legal, contractual, or some other kind of organisational arrangement, or informal, depending essentially on the strength of interpersonal trust and relationships. In defining networks and nodes, boundaries play an important role and must be explicitly delimited to avoid endless – and potentially meaningless – webs of connections. Confusing interpretations about the nature of nodes can also result from insufficiently well-defined boundaries. For example, large nodes – such as Interpol or Europol – can become networks in their own right when they reach a certain level of complexity. At the other end of the spectrum, particular individuals can play key roles in institutional networks, especially when these individuals broker relationships across organisational boundaries. There is no perfect solution to this methodological dilemma, but to avoid confusion authors should clearly define nodes and ties in security network research. Although a majority of the literature highlights the horizontal or egalitarian features of networks over their internal, potentially hierarchical tensions, significant variation in node capacity and power imbalances means that there will invariably be unequal relations in certain networks. In some contexts, such as in the organisational and public management literature, the concept of network has a much more precise meaning. For example, in one of the most influential papers in the field, Provan and Kenis (2008, p. 232) define a network as 'groups of three or more legally autonomous organisations that work together to achieve not only their own goals but also a collective goal'.

The network concept is used in three principal ways. The first – and most common – is as a *metaphor*, where a loose use of network terminology suggests some kind of self-organising relationships between a given set of nodes that operate in fragmented, fluid and complex environments (Knox *et al.* 2006). The use of the network term moves beyond a metaphor when researchers describe and analyse such factors as which actors comprise the particular network under analysis, the nature of the relationships between actors and how that network operates.

The second use relates to *network analysis*. SNA is a set of formal analytical tools widely used across the social and behavioural sciences (Wasserman and Faust 1994, Freeman 2004, Borgatti *et al.* 2013). While network analysis has been used extensively in relation to dark networks (e.g. Morselli 2009, 2014, Bouchard 2015), very few have applied it to 'bright' networks – those that are both licit and apparently more 'visible' – in the field of policing and security (Dupont 2006, Brewer 2014, Nøkleberg 2016). The limited number of empirical studies that apply the SNA toolbox to security issues reflects the methodological challenges associated with this approach. That is, contrary to dark networks, where data sets are more easily collected online or may be obtained from law enforcement or intelligence agencies, and bright networks in other fields such as public administration and management, mapping security networks usually requires high degrees of trust to broker access to respondents and thus significant resources at the data collection stage.

The third use refers to networks as a particular logic of organisation or *governance*. Such research largely reflects developments in organisation science and public administration (Jones *et al.* 1997, Provan and Kenis 2008, Popp *et al.* 2014, Molin and Masella 2016), where the network concept is used to refer to organisational configurations in which organisations constitute nodes and various formal exchange relations constitute ties. Whether a unique form of social organisation or a hybrid between hierarchies and markets (Powell 1990), networks are increasingly being used as platforms for organisations to work together to achieve their own goals and also shared goals. Networks often form as an attempt to address so-called 'wicked problems' (Rittel and Webber 1973), or those problems that cannot be formulated easily or divided into simple pieces that can be allocated to independent organisations, because they rely on often contradictory professional and political judgments for resolution (O'Toole 2007). Network forms of governance have been examined

across the security field in the context of actual security networks, where case studies have for example been conducted on business improvement districts (Sleiman and Lippert 2010), international police cooperation mechanisms (van Buuren 2012), or national security arrangements (Whelan 2012), to name a few. Very few scholars have drawn on the management literature to raise questions about the organisational properties of security networks (e.g. Whelan 2012, Giacomantonio 2014).

Our findings reveal that the metaphorical use of the term 'network' accounts for a significant share of the literature – 37% of the contributions we analysed. For example, researchers have drawn on the concept of network to identify security apparatuses where a diversity of actors interact on a regular basis to prevent street crime or fight terrorism (e.g. Brodeur and Dupont 2006, Crawford 2006, Bures 2013). Network, then, is used to suggest that relationships exist between a given set of actors that cooperate to achieve a common end. Researchers have concentrated much less on actual networks and very few have undertaken a comprehensive analysis of a 'whole' network (Provan *et al.* 2007). Many of these studies make limited use of the broader network literature.

The more empirically oriented papers adopt a goal-directed approach of networks (40%) or, to a lesser degree, an emergent approach (23%), a classical distinction in management studies (Kilduff and Tsai 2003). The goal-directed category includes studies on entities that recognise themselves as networks (e.g. Cherney *et al.* 2006, Palmer and Whelan 2006, Groenendaal and Helsloot 2015), work together to achieve their own goals as well as a broader collective goal, and have boundaries that are already well delimited by members themselves. These networks may employ a core-periphery design (Kilduff and Tsai 2003), where members of the core share an interest in the general goals of a particular network while other members reside on the periphery and come in and out of the core as the need arises in relation to a specific, often temporary, goal. This configuration would, for example, apply to an anti-money-laundering network where the core would consist of key law enforcement, regulatory and intelligence agencies, while the periphery would be made up of banks' internal security units and various private intelligence providers whose expertise would be mobilised in an *ad hoc* manner for specific cases. The emergent category focuses on communities of actors that often develop serendipitously and can be examined through a network lens but are not necessarily aware that they are embedded in a unified web of ties (e.g. Dupont 2006, Bénit-Gbaffou 2008, Levi and Williams 2013). Research projects on such emergent security networks require significant data collection efforts as researchers must identify relevant organisational actors in various fields of practice and then design methodologies that can capture sprawling relational patterns.

When we broke the terminology down even further, although all the documents comprising our database refer extensively to the network concept, only a little more than half (56%) actually focus on *networks* in one of the three specific ways outlined above, while 26% of the papers are more accurately described as focusing on *partnerships* – most notably the dynamics of relationships between public and private stakeholders. Contributions that use a partnership lens tend to rely on a more normative approach, examining the benefits and challenges of collaboration or, in some instances, its perils (e.g. Jameson and Strudwick 2009, Desmond and Valdez 2012, Cook 2013). The remainder (18%) evoke the language of network and/or partnership in the context of broader conceptual frameworks such as community policing (e.g. Baker 2009, Marks *et al.* 2009), third-party policing (e.g. Ransley and Mazerolle 2009, Drew 2011), governance of security (e.g. Fleming *et al.* 2006, Friesendorf 2007), plural policing (e.g. McCahill 2008, O'Reilly 2015) and police work (e.g. Cotter 2015).

The prevalence of studies with a goal-directed or metaphoric view of security networks as well as the blurred boundaries between security networks and partnerships or related concepts explain why qualitative methods such as interviews, focus groups, observations, life histories, document analysis and literature reviews dominated the methodological landscape – 80% of reviewed papers. Studies that relied exclusively on quantitative approaches such as surveys accounted for only 4% of our sample, while mixed methods were used in 16% of studies. This result is hardly surprising, as the systematic collection of quantitative data is a time-consuming task that entails much larger costs and efforts than the more focused node-centric approach allowed by qualitative methods. Reviews of

the management literature have made a similar observation, noting that many studies approach networks from the perspective of one single focal organisation (what network analysis calls an 'ego network') rather than studying the network as a whole (Provan *et al.* 2007). We suggest mixed methods is a promising compromise for capturing rich and complementary data at the node and network levels (Creswell 2014). This approach can enable researchers to both map security networks and their ties as well as more fully appreciate their underlying organisational dynamics.

Network forms

Beyond a review of epistemic approaches, we were also interested in understanding what types of networks have been studied. We focus on their geographical location and scope, their institutional make-up, the nature of ties under study, and the security issues addressed. The aim was to identify patterns that could suggest whether the network form tends to fit best with specific domains or regions as well as to locate notable clusters or gaps in the literature.

From an operational perspective, the level of diversity is extensive. Research has been conducted on networks delivering security in fields as diverse as, for example, urban security (e.g. Huey 2008), counter-terrorism (e.g. Gill 2006, Palmer and Whelan 2014), general policing (a category that focuses on basic policing tasks rather than on a particular geographical setting; e.g. Roberts and Roberts 2009), cyber-crime (e.g. Nhan and Huey 2008), high policing (e.g. O'Reilly and Ellison 2006), organised crime (e.g. Bruns 2015) and transport security (e.g. Paes-Machado and Nascimento 2014). However, Table 2, which summarises the distribution of papers across security issues, reflects the prominence of two themes that account for more than half of the sample. Urban security probably owes its first place to the more easily observable nature of the web of uniformed security providers, surveillance technologies and crime prevention strategies in modern cities, while counter-terrorism has come to be firmly anchored in the isomorphic belief that it takes a network to fight a network (Dupont 2015). Research on natural candidates for security network case studies such as emergency management, transport security, organised crime policing, or cyber-crime policing can be conducted only when researchers have significant resources and privileged access, which likely explains why it remains sporadic.

The institutional makeup of the security networks studied in our sample overwhelmingly favoured hybrid relationships between public, private and community stakeholders (81%), with a residual 19% dealing with exclusively public security networks. Not a single contribution studied a security network

Table 2. Distribution of the security issues dealt with by 117 security networks studied.

Issue	Number	%
Urban security	46	39.32
Counter-terrorism	16	13.68
General policing	13	11.11
Cyber-crime	7	5.98
High policing	4	3.42
Transport	4	3.42
Organised crime	4	3.42
Mega-event	4	3.42
Drug control	4	3.42
Police socialisation	2	1.71
Campus security	2	1.71
Emergency management	2	1.71
Border security	2	1.71
Human trafficking	1	0.85
Resource extraction	1	0.85
Health	1	0.85
Rural security	1	0.85
Various	3	2.56
Total	117	100

made up of private actors. Even O'Reilly (2010, 2015), one of the few to study transnational security consultancies that epitomise the growing capacity of corporate actors to perform high policing tasks outside government, inevitably reminds us of the symbiotic ties these players maintain with state security and intelligence agencies.

A classic way to understand networks is through the distinction between 'formal' and 'informal' ties. Most papers in our sample (87%) study both formal and informal ties, with 7% considering only formal and 6% only informal, but the inter-relationship between these types is rarely clearly identified. While informal ties often underpin formal networks, considerable work remains to be done to unpack the distinction between formal and informal ties and determine what distinguishes them and how they complement each other. For example, ties between two people from separate organisations ('boundary spanners') could have multiple functions – interpersonal and inter-organisational relationships, informal and formal – and it can be quite difficult to determine how one shapes another.

Dupont's (2004) typology devotes considerable attention to the geographical dimension of security networks, differentiating local, national and transnational configurations. Given the importance of the theme of urban security in this literature, it seems logical that subnational networks, which include local and regional groupings, account for 61% of the papers reviewed. An additional 21% were dedicated to national security networks and a more modest 14% focused on international networks. The empirical constraints created by arduous data collection procedures at the national and international levels may partly explain this distribution. In many instances, the categorisation process raised definitional challenges as, for example, when very local community policing networks are supported and funded by international organisations (e.g. Blaustein 2014). Finally, analysis of the countries of origin of the security networks studied (Table 3) illustrates that research in this area remains anchored in English-speaking social science communities, with a very strong presence of North American scholars. This situation may result from the fragmentation of security organisations caused by the highly decentralised US and Canadian federal systems and the proliferation of private security providers, which vastly outnumber public police officers in these two countries (Brodeur 2010), as both foster a greater need for networked coordination mechanisms. Other nations making cameo appearances include European countries (Greece and Norway), English-speaking African countries (Kenya, Liberia, Nigeria, Sierra Leone and Soudan), Latin-American countries (Argentina and Brazil) and Asian countries (China, India and Japan). The geographical coverage of this literature is unquestionably uneven and would certainly benefit from a more systematic research programme that would expand and diversify our empirical knowledge base.

A revised typology of security networks

We begin our review of questions about the dynamics, size and scope of networks by revisiting Dupont's (2004) typology of security networks, which concentrates largely on the geographical

Table 3. Countries of origin for the security networks studied.

Country	N^a	%
US	48	41.03
Canada	22	18.80
UK	18	15.38
Australia	18	15.38
South Africa	10	8.55
The Netherlands	7	5.98
Ireland	6	5.13
France	3	2.56
Other	30	25.64

[a]Certain studies examined networks operating in more than one country. The sum of countries of origin is therefore larger than 117 and percentages are greater than 100.

parameters in which networks operate and on membership across public, private and hybrid sectors. Dupont identified four ideal-types of *formal* security networks: local, institutional, international and virtual. While local and international security networks can clearly be distinguished in geographical scope, they also differ in terms of goals, nature of ties and dynamics. For example, local networks are directed toward local security problems and therefore almost always include public and private actors as well as physical ties. International security networks focus on cross-border security problems, are more likely to be state-based – with only a few including private actors – and to depend more on virtual ties.

The remaining two network types are not necessarily geographically focused but rather are defined more in terms of their functional or operational characteristics. Institutional security networks are referred to as those networks in which the explicit purpose is 'the facilitation of inter-institutional bureaucratic projects or the pooling of resources across government agencies' (Dupont 2004, p. 80). Such networks are exclusively state-based in terms of membership and are largely national in terms of scope. Examples include crime and security intelligence fusion centres (Monahan and Palmer 2009, Ratcliffe and Walden 2010, Chermak *et al.* 2013). Dupont initially suggested that institutional networks were mostly designed to maximise efficiency, but it is now recognised that some are intended to increase effectiveness, such as attempting to address complex or wicked problems. Virtual security networks are the technological systems that facilitate the communication and exchange of data and information between security nodes. Examples of these include the various intra- and inter-organisational databases that are designed to process data, information and intelligence between security actors. There are literally thousands of those systems and databases in operation in North America, Europe, Australasia and the rest of the world, across the field of policing and security.

While these four ideal-types are not exclusively geographically focused, they can be combined with our findings from the review of security network literature to create a revised typology, as summarised in Table 4.

Table 4 summarises some of the different features of security networks at the subnational, national and transnational levels. While it was helpful originally to categorise virtual networks as a distinct ideal-type, the prominence of technological systems in security networks at all levels suggests it is more useful to concentrate on the nature of network ties than to see virtual networks as a separate category. Many, if not most, security networks will involve both physical and virtual ties, especially if they are more formal and enduring in nature. Dupont's (2004) institutional security networks are replaced by networks operating at the national level, which provides flexibility for when non-state actors are permitted or required (as the case may be) to enter these particular security networks. Examples of this include telecommunications companies and financial institutions, which are playing increasing roles in combatting organised crime and terrorism (Michaels 2008, Amicelle 2011), and technology firms that are central players in cyber security (Dupont 2016).

We have extended the table to include key questions about network goals, membership, ties and dynamics to emphasise some of the important differences between networks with regard to *modus operandi* and particular structural and relational dynamics. We have also called attention to different capacities and constraints. For example, information classification requirements are unlikely to come into play at the local level whereas they almost certainly will, to varying degrees, in national and transnational security networks. As such, in order to better appreciate the membership and dynamics of security networks, we also need to consider where each network sits along the low-high policing continuum (Brodeur 2010). It is also important to recognise that leadership within networks may display various tensions.

This brings us to the limitations of a geographical-based typology of security networks. For instance, it was often assumed that a network's mode of exchange moves from the local to the international, through the national. Many local security actors have formed direct networks with their equivalents in other jurisdictions to share capabilities, development and training programmes, for

Table 4. Networks across the security field.

Network scope	Network goals	Network membership	Network ties	Network dynamics
Subnational	Local crime and security problems within defined territorial or jurisdictional boundaries Networks are typically goal-oriented but these goals may only be loosely stated	Membership is usually open to public and private security nodes Limited security classification constraints restricting membership	Ties are usually physical as in structured meetings, with support of some virtual systems Informal ties play a prominent role due to physical and institutional proximity	Leadership can shift between public and private actors although local police will often adopt central positions Relationships largely shaped by individual members on an interpersonal basis
National	National crime and security problems, or those crossing intra-national borders. These include (but are not limited to) organised crime, drug trafficking and terrorism Networks are largely goal-oriented with articulated objectives and often outcome-focused	Membership is usually limited to public security nodes, with private actors involved on the periphery on a case-by-case basis, mainly as a source of intelligence Medium to high security classification constraints restrict membership and mode of operations	Ties are both physical and virtual in nature, including structured meetings, liaisons, fusion centres and intelligence databases	Leadership can be a source of tension as security nodes often consider themselves to be equals and wield significant political influence Relationships shaped by inter-organisational and interpersonal dynamics
Transnational	Transnational crime and security problems or those crossing national borders Networks are goal-oriented with articulated objectives and strict modes of governance	Membership includes supranational and public security nodes with private actors involved on the periphery on a case-by-case basis, especially when they display unique forms of technical expertise High security classification constraints restrict membership and mode of operations	Ties are both physical and virtual, but more often facilitated by liaisons and information and communication systems	Leadership can vary between lead-country or lead-organisation depending on the nature of the task and network Relationships shaped by international and inter-organisational dynamics

instance. Examples include knowledge sharing arrangements between host jurisdictions of mega-events (Boyle 2011) as well as owners and operators of critical infrastructure such as port security (Brewer 2014). More relevant to our objectives in this paper, a geographical typology does not do justice to the myriad of *functions* that networks may perform. To better acknowledge the complexities of security networks, we propose a functional typology that would allow us to be more flexible and less constrained when dealing with networks that simultaneously operate across various geographical scales. For example, when international organisations fund local security networks to enhance community safety or when national police services pool their resources with multinational corporations to take down an international cyber-crime ring, traditional geographical boundaries are blurred and seem less relevant than the functions that are being fulfilled. Although there are very few attempts to develop typologies of organisational networks, those that do exist are largely based on network goals and functions. In the field of public administration and management, Milward and Provan (2006) distinguish between four main types of networks – those involved with service implementation, information diffusion, problem-solving and community capacity building. Another approach differentiates between outreach, informational, developmental and action networks (McGuire 2006). Other more extensive reviews have identified up to 20 different network types, albeit with considerable overlap between them (Popp *et al.* 2014). While it must be emphasised

that all security networks are potentially unique, with their own opportunities and constraints, it is still possible to distinguish some of the main functions performed by different networks.

We argue that four network types have considerable relevance across the security field and provide avenues for future research: information exchange networks, knowledge generating networks, problem-solving networks and coordination networks (see Table 5). Each of these forms can be identified at the subnational, national and transnational levels. Each of these types operates across the security field, with membership, nature of ties and dynamics varying in accordance with each network's specific goals and operational requirements. As with most typologies, there is overlap between the different forms and none is mutually exclusive. It is important to recognise as well that networks can have multiple functions. For example, all networks involve information sharing but in some instances this may be the primary goal in and of itself, while in other instances information is shared in order to achieve a particular purpose, such as generating knowledge, solving problems, or coordinating roles and responsibilities among organisations. A network that starts out as an information exchange may become a problem-solving network. These network types can therefore reasonably be expected to function in different ways and have potentially very different criteria for determining success.

Ultimately, distinguishing between different types of networks is useful only if it helps bring into focus the underlying purpose behind any particular network, which enables researchers and practitioners to better understand and analyse how networks form and function – both in a descriptive and prescriptive capacity. It is in this context that we present this typology here, particularly as a means of potentially sharpening the focus of future research on security networks. At present, much more security network research has concentrated on information sharing networks and, to a lesser extent, coordination networks than knowledge and problem-solving networks. However, as the remainder of this paper will show, we suggest all four types would benefit from further research.

A research agenda on security networks

Our review highlighted several areas that we believe require further attention by scholars who adopt a security network approach. In putting forward these suggestions we are sensitive to the various critiques of the network perspective in other contexts. For example, Dowding (2001, p. 89), in a paper critical of the policy network framework, expresses his scepticism about some of the findings in this literature, which in his view 'merely demonstrate what most of us would intuitively believe from more casual, nonformal observation'. His aim is not to discard network analysis but to remind the reader that this expensive and time-consuming methodology needs to be used discerningly to demonstrate how particular forms of organisation influence practices and policy outcomes, and to help explicate the nature of governance (Dowding 2001, p. 103). Other critiques in the organisational and management literature have argued that, although there is compelling

Table 5. Security network type and functions.

Network type	Network function
Information exchange networks	Facilitate the sharing of information across intra- and inter-organisational boundaries. Examples include automated police systems and crime intelligence databases
Knowledge generating networks	Generate new knowledge (understood as processed information enabling decision-making) and to distribute this knowledge between organisations. Examples can best be identified in relation to organised crime and terrorism threat assessments. Evidence-based policing networks that seek to identify and disseminate best-practices also belong to this category
Problem-solving networks	Develop responses to complex or 'wicked' problems that cannot be addressed by organisations acting alone. Examples include local security networks focusing on crime prevention initiatives to reduce gang violence (Boston's Operation Ceasefire, for example) or third-party policing interventions to improve quality of life
Coordination networks	Coordinate joint responses and service delivery across organisational boundaries. Examples can include joint police taskforces as well as can be identified in the field of disaster and emergency management

evidence that networks matter (Brass *et al.* 2004), researchers need to continue working to advance network theories of organisational behaviour, especially if we are to properly understand their normative aspects (Galaskiewicz 2007). We now aim to provide directions around the use of the network concept and method in the security network literature, and then identify pressing areas for further research on networks across the security field.

Research on security networks would benefit greatly from increased clarity and consistency in the use of the network concept. Much of literature reviewed adopts the network term as simply a metaphor to denote some kind of relationship, or set of relationships, between any given set of security actors. Actors or nodes and the nature of these relationships or ties are rarely explicitly defined. This is not the case in many other disciplines such as organisation and management studies, where a sophisticated literature has developed on various forms of networks. To advance the security network approach, we need to move beyond the metaphorical use of the concept and develop rigorous language to deal with specific types of networks and the ways nodes are networked. Some of the network language from other disciplines has great potential to assist with this task. For example, Kilduff and Tsai's (2003) distinction between goal-directed and emergent or serendipitous networks offers much promise to help distinguish between broad categories of networks and to determine how networks form and function. In defining goal-directed networks, we suggest that security network scholars follow the existing network literature (e.g. Provan and Kenis 2008) by defining networks as groups of three or more actors that work together to achieve independent and shared goals. Emergent networks, by contrast, follow a serendipitous trajectory that capitalises on opportunity and may rapidly change. The types of networks proposed above – information exchange, knowledge generating, problem-solving and coordination – also provide tools for differentiating between network types based largely on their goals and purpose.

To move away from the metaphorical use of the network term and address these research questions, scholars must adopt an appropriate methodological position. SNA clearly holds much promise as it enables researchers to map the relationships between a given set of actors and then apply various mathematical techniques to determine the nature of these relationships for individual actors as well as whole networks (Borgatti *et al.* 2013). Network analysis can be employed in virtually all circumstances to advance our knowledge of how networks function. With goal-directed networks, especially where membership is relatively stable, methods such as SNA can be used to describe and analyse the structural and relational properties of networks, which can then be juxtaposed against the network's stated goals. This is particularly useful for information sharing networks for example, where SNA is able to identify potential gaps or blockages in the flow of information. Even in serendipitous network types, SNA is useful for explaining how networks form and function at a specified point in time. Such an approach poses many methodological challenges – collecting relational data can be difficult in many security environments (Brodeur and Dupont 2006) and determining a network's boundaries is one of the main challenges with both dark and bright networks (Burcher and Whelan 2015) – but, as mentioned above, there are ways to address problems with data collection and adopting clear boundary specification rules can keep network studies to a workable level. We lack the space in this article to detail the actual methods that may be deployed to apply formal SNA techniques to security networks – and their strengths and limitations – but a growing number of manuals tailored to the particular needs and research questions of various disciplines provide excellent introductions (Wasserman and Faust 1994, Knoke and Yang 2008, Borgatti *et al.* 2013, Scott 2017).

Another approach is to draw more on the organisational or network governance literature that has flourished in fields such as public administration and management (e.g. Popp *et al.* 2014, Hu *et al.* 2015). This literature provides further concepts and tools to examine important network questions, particularly the factors shaping the effectiveness of networks and techniques for promoting their accountability (Kenis and Provan 2009). This approach is ideal for the remaining network types here – particularly knowledge sharing and problem-solving networks – as it is difficult to properly assess how these networks function and to what extent they achieve their goals via methods such

as SNA alone. Examining such networks requires researchers to 'look inside their operations' (Agranoff 2006, p. 56), which is an invaluable way to improve security network research. As other recent reviews of network research have found (Kapucu *et al.* 2014), however, mixed-methods research designs are highly likely to have the most potential for advancing security network research. Researchers can leverage the quantitative techniques of network analysis contextualised within a qualitative framework concerning the type of network under analysis, its specific goals and dynamics.

Once issues around terminology and methodology are addressed, there are many research questions worthy of further analysis. Due to space constraints, we limit our focus here to three observations. First, we need more research on specific security networks in various contexts, including countries – the vast majority of the literature is focused on North America – and across the low-high policing continuum. Such research is necessary to develop a body of literature that is sufficient for comparative research as well providing a knowledge base that will make it possible to understand and analyse the effects of culture, history and particular institutional configurations on networks (Brass *et al.* 2004). Second, further research should concentrate on the structural and relational properties of security networks and how these interact. Structural properties include attributes such as the design, size and level of goal consensus between network members (Provan and Kenis 2008). Relational properties refer to the relationships between actors within networks, including the potential for conflict and different levels and kinds of commitment among actors (Meyer and Mazerolle 2014, Whelan 2016, 2017). These properties interact continually, shaping network dynamics and the attributes of individual actors. Understanding these complex dynamics would help us better evaluate the evolution of a security network over time. Third, we need to move beyond purely descriptive accounts and develop more advanced ways of assessing the effectiveness and performance of security networks, using networks as both independent and dependent variables. Researchers should concentrate on what makes security networks effective and what causes them to fail (Yar 2011), not only as independent units of analysis but in relation to community or society expectations of what specific types of networks should and should not do. If we accept that networks are central to security governance, such a task is crucial to promoting security.

Conclusion

This article has provided a systematic review of the security network literature over the last decade to assess the state of such research since the publication of Dupont's (2004) initial programmatic paper on security networks. We focused on the types of security networks that have been studied, the terminology and methods employed to study them, and opportunities for further research. Noting the inconsistencies in terminology across the security network literature, we have argued strongly for a more exact and meticulous use of the network concept. We hope that limiting the network concept to groups, emphasising the distinction between goal-directed and emergent or serendipitous networks, and taking into account the different network types and functions put forward in this article will assist in this task. While it is unfortunately beyond the scope of this paper to develop this typology any further, we suggest that distinguishing between these four network types provide useful avenues to think about further research on specific security networks. By drawing on the analytical and organisational methodologies, we also hope that research will focus on the precise ways in which security nodes are networked and the structural and relational dynamics of these actual (rather than metaphorical) networks. This task is undoubtedly best achieved using mixed-methods approaches, but we recognise that this is not an easy process for many researchers. It is certainly possible, however, as the wider social and organisational network literature demonstrates. If there is a final conclusion, it is that there is compelling evidence across the security field that networks have become as important as hierarchies and markets. However, much more methodologically rigorous work is needed in a variety of contexts to advance our knowledge of how security networks form and function.

Acknowledgements

The authors would like to thank Emily Maddocks for her outstanding research assistance, as well as the participants to the Seventh Annual Illicit Networks Workshop, Peter Manning, James Sheptycki and Jennifer Wood, and the anonymous reviewers, for their helpful feedback on an earlier version of this article.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Agranoff, R., 2006. Inside collaborative networks: ten lessons for public managers. *Public administration review*, 66 (1), 56–65.

Amicelle, A., 2011. Towards a 'new' political anatomy of financial surveillance. *Security dialogue*, 42 (2), 161–178.

Ayling, J., Grabosky, P., and Shearing, C., 2009. *Lengthening the arm of the law: enhancing police resources in the twenty-first century*. Cambridge: Cambridge University Press.

Baker, B., 2009. A policing partnership for post-war Africa? Lessons from Liberia and Souther Soudan. *Policing and society*, 19 (4), 372–389.

Bayley, D. and Shearing, C., 2001. *The new structure of policing: description, conceptualization, and research agenda*. Washington, DC: National Institute of Justice.

Benkler, Y., 2006. *The wealth of networks: how social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Blaustein, J., 2014. The space between: negotiating the contours of nodal security governance through 'Safer Communities' in Bosnia-Herzegovina. *Policing and society*, 24 (1), 44–62.

Bénit-Gbaffou, C., 2008. Unbundled security services and urban fragmentation in post-apartheid Johannesburg. *Geoforum*, 39 (6), 1933–1950.

Borgatti, S., Everett, M., and Johnson, J. 2013. *Analyzing social networks*. London: Sage.

Bouchard, M., ed., 2015. *Advances in research on illicit networks*. New York: Routledge.

Bourdieu, P., 1986. The forms of capital. *In*: J. Richardson, ed. *Handbook of theory and research for the sociology of education*. New York: Greenwood Press, 241–258.

Boyle, P., 2011. Knowledge networks: mega-events and security expertise. *In*: C. Bennett and K. Haggerty, eds. *Security games: surveillance and control at mega-events*. Hoboken: Routledge, 169–184.

Brass, D., *et al.*, 2004. Taking stock of networks and organizations: a multilevel perspective. *Academy of management journal*, 47 (6), 795–817.

Brewer, R., 2014. *Policing the waterfront: networks, partnerships and the governance of port security*. Oxford: Oxford University Press.

Brodeur, J.-P., 2010. *The policing web*. Oxford: Oxford University Press.

Brodeur, J.-P. and Dupont, B., 2006. Knowledge workers or "knowledge" workers? *Policing and society*, 16 (1), 7–26.

Bruns, M. A network approach to organized crime by the Dutch public sector. *Police practice and research*, 16 (2), 161–174.

Buerger, M. and Green Mazerolle, L., 1998. Third-party policing: a theoretical analysis of an emerging trend. *Justice quarterly*, 15 (2), 301–327.

Burcher, M. and Whelan, C., 2015. Social network analysis and small group 'dark' networks: an analysis of the London bombers and the problem of 'fuzzy' boundaries. *Global crime*, 16 (2), 104–122.

Bures, O., 2013. Public-private partnerships in the fight against terrorism? *Crime, law and social change*, 60 (4), 429–455.

Castells, M., 1996. *The information age: economy, society and culture, Vol. 1: the rise of the network society*. Cambridge: Blackwell.

Castells, M., 2000. Material for an exploratory theory of the network society. *British journal of sociology*, 51 (1), 5–24.

Castells, M. and Cardoso, G., eds., 2005. *The network society: from knowledge to policy*. Washington, DC: Johns Hopkins Center for Transatlantic Relations.

Chermak, S., *et al.*, 2013. Law enforcement's information sharing infrastructure: a national assessment. *Police quarterly*, 16 (2), 211–244.

Cherney, A., O'Reilly, J., and Grabosky, P. 2006. Networks and meta-regulation: strategies aimed at governing illicit synthetic drugs. *Policing and society*, 16 (4), 370–385.

Cook, I., 2013. Policing, partnerships, and profits: the operations of business improvement districts and town center management schemes in England. *Urban geography*, 31 (4), 453–478.

Cotter, R., 2015. Police intelligence: connecting-the-dots in a network society. *Policing and society*, 27 (2), 173–187.

Crawford, A., 2006. Networked governance and the post-regulatory state? Steering, rowing and anchoring the provision of policing and security. *Theoretical criminology*, 10 (4), 449–479.

Creswell, J., 2014. *Research design: qualitative, quantitative and mixed methods approaches*. Thousand Oaks, CA: Sage.

Desmond, M. and Valdez, N., 2012. Unpolicing the urban poor: consequences of third-party policing for inner-city women. *American sociological review*, 78 (1), 117–141.
Dowding, K., 2001. There must be end to confusion: policy networks, intellectual fatigue, and the need for political science methods courses in British universities. *Political studies*, 49 (1), 89–105.
Drew, J., 2011. Police responses to the Methamphetamine problem: an analysis of the organizational and regulatory context. *Police quarterly*, 14 (2), 99–123.
Dupont, B., 2004. Security in the age of networks. *Policing and society*, 14 (1), 76–91.
Dupont, B., 2006. Delivering security through networks: surveying the relational landscape of security managers in an urban setting. *Crime, law and social change*, 45 (3), 165–184.
Dupont, B., 2014. Private security regimes: conceptualizing the forces that shape the private delivery of security. *Theoretical criminology*, 18 (3), 263–281.
Dupont, B., 2015. Security networks and counter-terrorism: a reflection on the limits of adversarial isomorphism. *In*: M. Bouchard, ed. *Social networks, terrorism and counter-terrorism*. New York: Routledge, 155–174.
Dupont, B., 2016. Bots, cops and corporations: on the limits of enforcements and the promise of polycentric regulation and as way to control large-scale cybercrime. *Crime, law and social change*, 67 (1), 97–116.
Fleming, J., Marks, M., and Wood, J. 2006. 'Standing on the inside looking out': the significance of police unions in networks of police governance. *The Australian and New Zealand journal of criminology*, 39 (1), 71–89.
Freeman, L., 2004. *The development of social network analysis: a study in the sociology of science*. Vancouver: Empirical Press.
Friesendorf, C., 2007. Pathologies of security governance: efforts against human trafficking in Europe. *Security dialogue*, 38 (3), 379–402.
Galaskiewicz, J., 2007. Has a network theory of organizational behavior lived up to its promises? *Management and organization review*, 3 (1), 1–18.
Giacomantonio, C., 2014. A typology of police organizational boundaries. *Policing and society*, 24 (5), 545–565.
Gill, P., 2006. Not just joining the dots but crossing the borders and bridging the voids: constructing security networks after 11 September 2001. *Policing and society*, 16 (1), 27–49.
Grabosky, P., 1995. Using non-governmental resources to foster regulatory compliance. *Governance: an international journal of policy and administration*, 8 (4), 527–550.
Groenendaal, J. and Helsloot, I., 2015. Toward more insight into the tension between policy and practice regarding the police network function of community police officers in the Netherlands. *Police journal: theory, practice and principles*, 88 (1), 34–50.
Hu, Q., Khosa, S., and Kapucu, N., 2015. The intellectual structure of empirical network research in public administration. *Journal of public administration research and theory*, 26 (4), 593–612.
Huey, L., 2008. When it comes to violence in my place, I am the police!' Exploring the policing functions of service providers in Edinburgh's Cowgate and Grassmarket. *Policing and society*, 18 (3), 207–224.
Jameson, J. and Strudwick, K., 2009. Tensions in security partnerships: observations of a city CCTV system and its partners on the ground. *Crime prevention and community safety*, 11 (2), 90–103.
Johnston, L. and Shearing, C., 2003. *Governing security: explorations in policing and justice*. London: Routledge.
Jones, C., Hesterly, W., and Borgatti, S. 1997. A general theory of network governance: exchange conditions and social mechanisms. *The academy of management review*, 22 (4), 911–945.
Jones, T. and Newburn, T., 1998. *Private security and public policing*. Oxford: Clarendon Press.
Jones, T. and Newburn, T., eds., 2006. *Plural policing: a comparative perspective*. London: Routledge.
Kapucu, N., Hu, Q., and Khosa, S. 2014. The state of network research in public administration. *Administration and Society* (online first 6 November 2014).
Kenis, P. and Provan, K., 2009. Towards an exogenous theory of public network performance. *Public administration*, 87 (3), 440–456.
Kilduff, M. and Tsai, W., 2003. *Social networks and organizations*. London: Sage.
Knoke, D. and Yang, S., 2008. *Social network analysis*. 2nd ed. Thousand Oaks, CA: Sage.
Knox, H., Savage, M., and Harvey, P. 2006. Social networks and the study of relations: networks as method, metaphor and form. *Economy and society*, 35 (1), 113–140.
Latour, B., 2005. *Reassembling the social: an introduction to actor-network-theory*. Oxford: Oxford University Press.
Levi, M. and Williams, M., 2013. Multi-agency partnerships in cybercrime reduction: mapping the UK information assurance network cooperation space. *Information management and computer security*, 21 (5), 420–443.
Loader, I., 1999. Consumer culture and the commodification of policing and security. *Sociology*, 33 (2), 373–392.
Loader, I. and Walker, N., 2007. *Civilizing security*. Cambridge: Cambridge University Press.
Marks, M., Shearing, C., and Wood, J. 2009. Who should the police be? Finding a new narrative for community policing in South Africa. *Police practice and research*, 10 (2), 145–155.
Mazerolle, L. and Ransley, J., 2006. *Third party policing*. Cambridge: Cambridge University Press.
McCahill, M., 2008. Plural policing and CCTV surveillance. *In*: M. Deflem and J. Ulmer, eds. *Surveillance and governance: crime control and beyond*. Bingley: Emerald Group, 199–209.

McGuire, M., 2006. Collaborative public management: assessing what we know and how we know it. *Public administration review*, 66 (1), 33–43.
Meyer, S. and Mazerolle, L., 2014. Police-led partnership responses to high risk youths and their families: challenges associated with forming successful and sustainable partnerships. *Policing and society*, *24* (2) 242–260.
Michaels, J.D., 2008. All the president's spies: private-public intelligence partnerships in the war on terror. *California law review*, 96 (4), 901–966.
Milward, H. and Provan, K., 2006. *A manager's guide to choosing and using collaborative networks*. Washington, DC: IBM Center for The Business of Government.
Molin, M.D. and Masella, C., 2016. From fragmentation to comprehensiveness in network governance. *Public organization review*, 16 (4), 493–508.
Monahan, T. and Palmer, N.A., 2009. The emerging politics of DHS fusion centers. *Security dialogue*, 40 (6): 617–636.
Morselli, C., 2009. *Inside criminal networks*. New York: Springer.
Morselli, C., ed., 2014. *Crime and networks*. New York: Routledge.
Nhan, J, and Huey, L., 2008. Policing through nodes, clusters and bandwidth. *In*: S. Leman-Langlois, ed. *Technocrime: Technology, crime and social control*. Portland, OR: Willan Publishing, 66–87.
Nøkleberg, M., 2016. Security governance – an empirical analysis of the Norwegian context. *Nordisk politiforskning*, 3 (1), 53–82.
O'Reilly, C., 2010. The transnational security consultancy industry: a case of state-corporate symbiosis. *Theoretical criminology*, 14 (2), 183–210.
O'Reilly, C., 2015. The pluralization of high policing: convergence and divergence at the public-private interface. *The British journal of criminology*, 55 (4), 688–710.
O'Reilly, C. and Ellison, G., 2006. Eye spy private high: Re-conceptualizing high policing theory. *British journal of criminology*, 46 (4), 641–660.
O'Toole, L., 2007. Treating networks seriously: practical and research-based agendas in public administration. *Public administration review*, 57 (1), 45–52.
Paes-Machado, E. and Nascimento, A.M. 2014. Conducting danger: practices and nodal networks of security governance among taxi drivers. *International journal of comparative & applied criminal justice*, 38 (1), 1–22.
Palmer, D. and Whelan, C., 2006. Counter-terrorism across the policing continuum. *Police practice and research*, 7 (5), 449–465.
Palmer, D. and Whelan, C., 2014. Policing and networks in the field of counter terrorism. *In*: D. Das, A. Turk, and D. Lowe, eds. *Examining political violence: studies of terrorism, counterterrorism, and internal war*. Boca Raton, FL: CRC Press, 145–166.
Popp, J., *et al.*, 2014. *Inter-organizational networks: a review of the literature to inform practice*. Washington, DC: IBM Center for the Business of Government.
Powell, W., 1990. Neither market nor hierarchy: network forms of organization. *Research in organizational behavior*, 12, 295–336.
Provan, K., Fish, A., and Sydow, J. 2007. Interorganizational networks at the network level: a review of the empirical literature on whole networks. *Journal of management*, 33 (3), 479–516.
Provan, K. and Kenis, P., 2008. Modes of network governance: structure, management and effectiveness. *Journal of public administration research and theory*, 18 (2), 229–252.
Raab, J. and Milward, H., 2003. Dark networks as problems. *Journal of public administration research and theory*, 13 (4), 413–439.
Rainee, L. and Wellman, B., 2012. *Networked: the new social operating system*. Cambridge: MIT Press.
Ransley, J. and Mazerolle, L., 2009. Policing in an era of uncertainty. *Police practice and research*, 10 (4), 365–381.
Ratcliffe, J. H. and Walden, K., 2010. State police and the intelligence center: a study of intelligence flow to and from the street. *IALEIA journal*, 19 (1), 1–19.
Rittel, H. and Webber, M., 1973. Dilemmas in a general theory of planning. *Policy sciences*, 4 (2), 155–169.
Roberts, A. and Roberts, J. M., Jr., 2009. Impact of network ties on change in police agency practices. *Policing*, 32 (1), 38–55.
Schuilenburg, M., 2015. *The securitization of society: crime, risk and social order*. New York: New York University Press.
Scott, J., 2017. *Social network analysis: fourth edition*. Thousand Oaks, CA: Sage.
Sleiman, M. and Lippert, R., 2010. Downtown ambassadors, police relations and 'clean and safe' security. *Policing and society*, 20 (3), 316–335.
van Buuren, J., 2012. Runaway bureaucracy? The European police chiefs task force. *Policing: a journal of policing and practice*, 6 (3), 281–290.
Wasserman, S. and Faust, K., 1994. *Social network analysis: methods and applications*. Cambridge: Cambridge University Press.
Wasserman, S. and Galaskiewicz, J., eds., 1994. *Advances in social network analysis: research in the social and behavioral sciences*. Thousand Oaks, CA: Sage.
Watts, D., 2003. *Six degrees: the science of a connected age*. New York: W. W. Norton.
Whelan, C., 2012. *Networks and national security: dynamics, effectiveness and organisation*. London: Routledge.

Whelan, C., 2016. Informal social networks within and between organisations. *Policing: An international journal of police strategies & management*, 39 (1), 145–158.
Whelan, C., 2017. Security networks and occupational culture: understanding culture within and between organisations. *Policing and society*, 17 (2), 113–135.
Wood ., J. and Dupont, B., eds., 2006. *Democracy, society, and the governance of security*. Cambridge: Cambridge University Press.
Yar, M., 2011. From the 'governance of security' to 'governance failure': refining the criminological agenda. *Internet journal of criminology*, 1–19.