Article

Surveillance, Security and Sports Mega Events: Toward a Research Agenda on the Organisation of Security Networks

Chad Whelan

Deakin University, Australia. chad.whelan@deakin.edu.au

Abstract

Surveillance and security at sports mega events have been the subject of considerable scholarly attention. Events such as the Olympic Games and Fédération Internationale de Football Association (FIFA) World Cups have become occasions of almost unparalleled economic, political and social significance. In the lead up to the London 2012 Olympic Games, scholars have examined issues such as the ‘security legacies’ of sports mega events, the infrastructures and technologies used in an attempt to secure these events, and the planning mentalities underpinning the staggering ‘security spectacle’ of these globally televised events. This paper deals with the subject of how surveillance and security practices at sports mega events are organised. It uses the emerging paradigm of ‘security networks’ to call attention to some important issues involving the entire ‘security assemblage’ that accompanies these mega events. The paper presents five levels of analysis—structural, cultural, policy, technological and relational—to examine these practices and documents several key areas for further research on sports mega events.

Introduction

Sports mega events such as the Olympic Games, Fédération Internationale de Football Association (FIFA) World Cups and Commonwealth Games have become occasions of unparalleled economic, political and social significance. However, ensuring security at these events has been a major ongoing concern since the 1972 Munich Games and appears to have taken on a new meaning since the events of 11 September 2001 (hereafter 9/11). This was clearly demonstrated recently with the London 2012 Olympic Games, which easily became the largest security operation to ever take place inside the United Kingdom. London 2012 was plagued with security concerns from the day the host city was announced by the International Olympic Committee, with the right to host the Games announced less than 24 hours prior to four suicide bombers attacking the Underground transport system, killing 52 people and seriously injuring hundreds more. As with the 1972 Munich Games—where the Olympic Village was infiltrated by a Palestinian group known as Black September that took 11 members of the Israeli Olympic team hostage who were later killed—the London bombings raised fears of sports mega events being considered an ideal ‘soft target’ to be exploited by potential terrorists. More recent events in which two bombs exploded close to the finish line of the Boston Marathon on 15 April 2013, killing three people and injuring over 250, have again highlighted that large scale sporting events are extremely difficult to secure, particularly where crowds congregate over wide and relatively open spaces. The Boston bombings have also shown the size and scale of the audience watching, which may further appeal to potential terrorists.

Over the decade since 9/11, security has grown exponentially at sports mega events. Giulianotti and Klauser (2010) highlight this trend in relation to the increasing economic costs of security measures and

Whelan, C. 2014. Surveillance, Security and Sports Mega Events: Toward a Research Agenda on the Organisation of Security Networks. *Surveillance & Society* 11(4): 392-404.
<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author(s), 2014 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

numbers of personnel. For example, the pre-9/11 security costs for the Olympic Games have increased from US\$179.6 million at Sydney 2000 to US\$1.5 billion for Athens 2004 and the exceptional case of US\$6.5 billion for Beijing 2008 (see Yu, Klauser and Chan 2009). Although exact expenditures are still unknown, it is estimated that the security costs for London 2012 were at least US\$950 million, despite the host city's already significant investments in security and surveillance infrastructure post the 7 July 2005 bombings and economic problems following the Global Financial Crisis (see Fussey and Coaffee 2012a). In terms of personnel, Sydney 2000 deployed approximately 5,000 police, 3,500 defence and up to 7,000 contract security staff (Lenskyj 2002) while London 2012 was initially asked to provide over 15,000 police, 13,500 defence force personnel and close to 15,000 contract security staff (Home Office 2011a, 2011b). Further, in the days leading up to the London 2012 Games, there was a significant addition of 3,500 defence personnel as concerns arose that G4S, the leading contract security provider, would not be able to supply the agreed number of private security staff (Hopkins 2012). This increased the total number of defence personnel to approximately 17,000, almost twice the number of troops then deployed in Afghanistan (Hopkins and Booth 2012). Indeed, Peter Ryan (2003: 24), former Commissioner of the New South Wales Police and now leading security advisor to the IOC, describes the task of securing sports mega events as 'impossible, complicated, difficult, challenging, complex and technologically advanced', noting that '[w]ars have been planned and executed in less time and with less people' (Ryan 2003: 23).

The lessons of 9/11 are particularly relevant to sports mega events, and clearly demonstrate the extent of the task of organising surveillance and security. For example, the 9/11 Commission Report (2004) concludes that 9/11 was not only an 'intelligence failure' but more accurately a failure to 'connect the dots'. Western governments have aimed to learn this lesson by improving their structures to promote greater cooperation, coordination and collaboration between departments and agencies involved in national security. The United States created the Department of Homeland Security, which amalgamated a series of pre-existing agencies, in an attempt to enhance inter-agency coordination. In countries like Australia, Canada and the United Kingdom, this has for the most part been pursued through formal and informal 'networks' designed to strengthen the pre-existing 'ties' between security agencies (Whelan 2012). Coordinating 'security networks' is challenging enough in routine operations (Dupont 2004; Gill 2006; Whelan 2012), but becomes even more challenging in the context of sports mega events. In the words of Ryan (2003: 26): 'as an exercise in testing cooperation, there is no better context than the Olympic security operation', emphasising that 'should an incident occur which could have been prevented by better communication and cooperation, the public will hold someone accountable'. In reflecting on these challenges for London 2012, Weston (2011: 202) briefly concludes that '[t]here is no doubt that the challenges of multi-agency coordination will be multiplied many times over by the magnitude of the Olympics'.

This paper contributes to a recent and growing body of literature concerning the intersecting issues of surveillance and security at sports mega events (e.g., Bennett and Haggerty 2011; Boyle and Haggerty 2009, 2012; Coaffee and Fussey 2010; Coaffee et al. 2011; Fussey and Coaffee 2012a; Giulianotti and Klausner 2010; Richards, Fussey and Silke 2011) by bringing attention to the important issue of 'security networks'. The paper proceeds in three sections. The first provides an overview of the concepts of 'surveillance' and 'security', building on recent work aimed at clarifying the relationship between these terms. While recognising that security and surveillance are related yet distinct concepts, *surveillance* is largely viewed in this paper as one of the key methods for trying to promote security at sports mega events. The second section seeks to unpack the relationship between security and surveillance by highlighting gaps in the current literature relating to the organisation of both practices of governance. The third section seeks to advance a research agenda focusing on the significance of security networks in securing sports mega events and outlines a framework for how these processes can be analysed. The paper concludes by suggesting that sports mega events and mass sporting events generally require ongoing research to examine the complex relationship between surveillance and security, which can be significantly advanced through taking a network perspective.

Security and Surveillance

Security and surveillance are related yet highly distinct concepts that are difficult to define with precision. In attempting to clarify the relationship between these terms, Lyon and Murakami Wood (2012) focus on distinguishing between ‘security’ and ‘surveillance’ by first briefly tracing the origins of Security Studies, as a sub-discipline of International Relations, and Surveillance Studies, as essentially a multi-disciplinary field of inquiry centred on the practices of surveillance. They illustrate how these fields overlap in theory and in practice, but strongly argue that security and surveillance need to remain distinct concepts. Security, they suggest, ‘speaks of a goal, an intended outcome, whereas surveillance speaks much more of a practice, method, or means’ (Lyon and Murakami Wood 2012: 321). They go on to explain that ‘security often requires surveillance but there are also other means by which security may be sought’ and that ‘[s]urveillance is often practiced in order to provide or procure security, but there are many additional purposes for which it may be applied’ (Lyon and Murakami Wood 2012: 322).

While this is a positive start there is more to consider when defining the concept of ‘security’ and, in turn, the relationship between security and surveillance. Security has traditionally been defined very narrowly by Security Studies, whereby the ‘referent object’ (Buzan, Waever and Wilde 1998) of security was the state and ‘existential threats’ were largely derived from other states. Despite the rise of other referent objects and existential threats such as ‘computer security’, ‘economic security’, ‘environmental security’, ‘food security’ and ‘human security’, Security Studies largely remains preoccupied with the notion of ‘national security’, although conceptualisations of this term have considerably broadened since 9/11 (Zedner 2009). Security is, as Zedner (2009: 10) argues, ‘too big an idea to be constrained by the strictures of any single discipline’. As such, one must look well beyond the field of Security Studies to truly understand the concept of security. The impact of this is significant. As Valverde (2011: 5) argues, ‘we think about security not as a thing, concept or condition but rather as an umbrella term under which one can see a multiplicity of governance processes that are dynamic and internally contradictory’. While accepting that there may not necessarily be anything grammatically wrong with using the term ‘security’ as a noun, Valverde (2011: 5) cautions that ‘it is dangerous to go on to the assumption that security actually exists, even as a fuzzy concept’. Therefore, care should be exercised when thinking of security as a ‘goal’ or ‘intended outcome’, even if this is implied by those invoking the term, because this risks confusing an ‘objective’ condition of security with the hypothetical state of ‘absolute security’ (Zedner 2009). Absolute security has a number of underlying assumptions, such as that it is predicated on knowledge of existential threats to one’s security, the static or unchanging nature of those threats and complete protection from such threats. Attention should also be devoted to the equally important conception of security as a ‘subjective condition’, which essentially holds that ‘security is all in the mind’ (Zedner 2009: 16). Ultimately, as Valverde (2011: 5) concludes, ‘all that we can know about security is what people do in its name’. In sum, should security be articulated as something closer to a ‘goal’ or ‘intended outcome’, as Lyon and Murakami Wood (2012) suggest, the attainment of security can only be assessed in terms of the extent to which these practices succeed in reducing or removing each known threat to a particular referent object. Security, like surveillance, is therefore a ‘practice’ rather than an end goal (see Zedner 2009). That is, regardless of how these practices of governance are performed, they are done with full knowledge that an actual objective condition of ‘security’ is ‘probably unattainable and at best impermanent’ (Zedner 2009: 19).

Surveillance can be defined in a similar way. For example, Lyon (2007: 14) defines surveillance as ‘the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction’. Lyon goes on to explain that surveillance is ‘focused’ on the personal details of individuals, ‘systematic’ to the extent that it involves the organised monitoring of individuals, and ‘routine’ in that it occurs as part of everyday life. Although exceptions to these general conditions apply, Lyon’s (2007: 15) main point is that ‘it is crucial to remember that surveillance is always hinged to some

specific purposes' of influencing or managing individuals and their behaviour. These purposes need not be malign or benign; they can be both and many varieties in between. Surveillance, in sum, is a 'practice' with a special 'purpose', such as to control or monitor populations. This idea fits neatly with the view that surveillance is fundamentally a 'social-ordering process' (Lyon, Haggerty and Ball 2012).

Both security and surveillance invoke very similar practices and are carried out for very similar purposes. For example, it is difficult to imagine any practices of security that do not involve at least some attempts to engage in the focused and systematic attention to the personal details of individuals for the purposes of influencing, monitoring or controlling their movements. However, while surveillance initiatives often extend beyond the purposes of security, such as in relation to protecting revenues of mega event organisers and promoters (Bennett and Haggerty 2011), their primary purposes in the case of sports mega events at least is intended to promote a condition of 'security'. Indeed, this is largely the focus of most recent sports mega event literature (see Giulianotti and Klauser 2011). In what follows, questions of surveillance are largely viewed as subsets of the broader security questions that apply to sports mega events.

Security, Surveillance and Sports Mega Events

Security and surveillance practices at sports mega events have attracted considerable attention leading up to the London 2012 Olympic Games. While some of this literature examines issues such as the globalisation of sport and sports governance (see Giulianotti and Brownell 2012), a significant proportion concentrates directly on the intersecting issues of security and surveillance (see Giulianotti and Klauser 2011). Much of the literature focuses on three overlapping issues: a) 'security legacies' of sports mega events (e.g., Bennett and Haggerty 2011; Coaffee et al. 2011; Fussey, Coaffee, Armstrong and Hobbs 2011; Fussey and Coaffee 2012b); b) security risks and the infrastructures and technologies used in an attempt to manage those risks (Fussey and Coaffee 2012a; Giulianotti and Klauser 2010, 2012; Richards et al. 2011); and c) the overall 'security spectacle' that characterises sports mega events (e.g., Boyle 2012; Boyle and Haggerty 2009, 2012; Coaffee et al. 2011). Each of these themes is now briefly considered in turn.

The security legacies of sports mega events have attracted considerable recent attention. A strong object of Surveillance Studies is how security and surveillance technologies, often initially implemented in an attempt to 'secure' sports mega events, continue to function post the event in everyday life, and with the familiar logic of 'mission creep' end up being used for other purposes than they were originally developed. Video-surveillance systems are a prime example (Bennett and Haggerty 2011). Giulianotti and Klauser (2010: 54) call attention to six security legacies of sports mega events: security technologies; new security practices; governmental policies and new legislation; externally imposed social transformations; generalised changes in social and trans-societal relationships; and urban redevelopment. For the most part, security technologies such as surveillance systems and urban redevelopment have been the focus of most critical attention (Coaffee et al. 2011), although analysts are increasingly examining the legacies of governmental policies and legislation. For example, Toohey and Taylor (2012) highlight some of the security legacies that followed the Sydney 2000 Olympic Games, including enhanced capacities for surveillance and legislative powers for police and security agencies to control and monitor behaviour at localised sports events (see also Taylor and Toohey 2011). More generally, the 'legacies' of London 2012, including new sports infrastructure and urban renewal, were put forward as major ongoing advantages of hosting the Olympic Games (Fussey, Coaffee, Armstrong and Hobbs 2012), which may in turn transform into lasting 'security legacies'.

Security risks, infrastructures and technologies encompass the ways in which risks to the security of sports mega events are identified and managed. Giulianotti and Klauser (2010) place these security risks in three categories: a) terrorism; b) spectator and political violence; and c) poverty, social divisions and urban

crime. While these risks vary according to the particular dynamics of the event and the host city, they are all considered as part of mega event security planning to varying degrees (e.g., Boyle and Haggerty 2012). Terrorism, for example, has been a key risk for every Olympic Games since the 1972 Munich Games regardless of the threat environment experienced in the host city (Fussey 2011; Fussey and Coaffee 2012b; Jennings 2011, 2012; Giulianotti and Klauser 2010; Manning 2006; Richards et al. 2011; Thompson 1996). A significant amount of resources is devoted to intelligence and surveillance activities targeting potential security risks in the lead up to any sports mega event. This was made clear in the security strategy for London 2012 (Home Office 2011a, 2011b).

In relation to how security risks are managed the overwhelming focus of recent literature is on the security infrastructures and surveillance technologies used to promote security. For example, Coaffee, Fussey and Moore (2011) trace the extent of the security operation for London 2012 and how it compares with some prior Olympic Games (see also Coaffee and Fussey 2010; Fussey and Coaffee 2012a, 2012b; Fussey et al. 2011). Uniquely positioned in terms of both the design of urban space and advanced surveillance technologies, Coaffee et al. (2011) describe how London implemented its version of the conventional Olympic ‘total’ security model. In addition to proactive policing and intelligence efforts being directed towards potential threats, key elements of the total security model included at least three key stages. The first involved intense planning for ‘resilience’ should the goal of ‘prevention’ fail and security problems such as a terrorist attack eventuate during the Games. The second involved reconfiguring public and private space into security infrastructures through the development of ‘island’ security and sophisticated ‘defensible space’ techniques at key sites. The third concerned the deployment of advanced surveillance and real-time monitoring of people and space, much of which involved expanding the existing network of surveillance technologies in the host city. These measures were also accompanied by an intense ‘military urbanism’ that played a crucial role in the overall ‘securitisation’ of the Olympic Games.

There is little doubt that many of these developments are about the ‘security spectacle’ rather than bearing a correlation to actual security risks. For example, the show of military ‘strength’ during London 2012—involving an aircraft carrier docked on the Thames, several RAF fighters, fixed long-range surface-to-air missiles deployed at several locations and portable missiles on the top of apartment buildings close to Olympic sites, Unmanned Ariel Vehicles or ‘drones’, and the more traditional positioning of tactical teams and snipers—would be considered far beyond any probable threat to the Olympics. Leaving aside the question as to whether these sorts of measures actually function as a genuine ‘deterrent’ to potential security risks, these initiatives are also as much about ‘subjective’ rather than ‘objective’ components of security. While some analysts have carefully questioned the rationale for such extreme responses to security, very few have actually addressed the ways in which decisions are made about how to secure and what to secure from. For example, Boyle and Haggerty (2012) argue that security spectacles and the planning for extreme events that underpins them are largely about providing the illusion of ‘absolute security’ and an attempt to control uncertainty. Others have focused on Olympic security as a ‘speech act’ (MacDonald and Hunter 2013), questioning the ways in which security problems are framed and communicated in line with the broader process of ‘securitisation’ (see Waever 1995; Loader 2002). Equally plausible, as Boyle and Haggerty (2012) suggest, is that while this enormous display of security may act as a possible deterrent and produce increased feelings of security for some, such extreme security measures can actually exacerbate feelings of ‘insecurity’ in others (Zedner 2009), particularly amongst the uninformed witnesses of the spectacle. For example, people can become anxious should they actually think about the need for all this ‘security’. This may have the added effect of amplifying surveillance and uncertainty rather than meaningfully enhancing overall levels of security (Boyle and Haggerty 2012).

Despite advancing our knowledge of security planning, infrastructures, surveillance technologies and their ongoing legacies after sports mega events have concluded, important questions remain in relation to precisely how all this ‘security’ can actually be coordinated. While virtually all analysts recognise that ‘sporting mega-events involve a level of organisation unmatched outside of wartime and planning that

requires significant alterations to the governance of the host city or country' (Fussey and Coaffee 2012a: 2), very few have sought to examine how security agencies and agents, which in the case of London 2012 numbered in excess of 40,000, are organised. In fact, it is also acknowledged that 'when security problems have occurred at sporting mega-events, it is the coordination and communication components that have proved to be both crucial yet are also the most common points of failure' (Fussey and Coaffee 2012a: 15). One of the few to address this problem is Boyle (2011, 2012), who briefly traces some of the issues concerning inter-agency coordination. While bringing attention to the issues of communication and institutional structures, and the ways in which event organisers have attempted to deal with these challenges, Boyle (2012) also makes the point that these are complex questions involving, *inter alia*, issues of expertise, culture and trust. These questions are fundamentally about 'networks' (Whelan 2012).

Security Networks and Sports Mega Events

The concept of 'network' has been used to call attention to the relationships between agents involved in policing and security. Although some have used the term loosely in relation to 'surveillance networks' (Lippert and O'Connor 2006), most have focused on 'security networks' (Brodeur and Dupont 2008; Dupont 2004, 2006; Gill 2006; Palmer and Whelan 2006, 2014; Whelan 2011, 2012). For example, Dupont (2004) distinguishes between different ideal-types of security networks, showing how they apply at the local through to the international levels. Gill (2006) analyses how security agents work together across different local, national and transnational 'levels' and state, corporate and communitarian 'sectors'. However, while the network concept is useful for 'mapping' the relationships (or 'ties') between security agencies (Dupont 2006), more work is needed in order to analyse and understand exactly *how* these agencies work together. Following the public administration and management literature (e.g., Provan, Fish and Sydow 2007; Provan and Kenis 2008), these networks can be conceived as deliberately structured platforms where agencies are required to work together to achieve their own goals as well as a broader collective goal. Understanding these networks is crucial in order to understand precisely how the practices of surveillance and security are organised. The remainder of this article defines 'networks' and 'security networks', and puts forward a framework for further analysis in relation to sports mega events.

Defining 'Networks' and 'Security Networks'

The term 'network' typically refers to a method of analysing relationships between a set of actors, or to a unit of analysis relating to a particular form of organisation or governance. In network analysis, a network can be defined as a set of actors or 'nodes' that have or may have relationships or 'ties' (Borgatti and Foster 2003; Porter and Powell 2006). Actors can be people, groups, or organisations, for example. Relationships can be of any type, and each type can define a different network. The idea of network analysis is to 'map' the pattern of relationships between actors and to analyse the implications of these relationships for the network and, more particularly, the *actors* in the network. Social network analysis has long been presented as a surveillance and intelligence gathering technique (Sparrow 1991; Klerks 1999). However, after 9/11 (Krebs 2002) it has been used to map security problems or 'dark networks' (Milward and Raab 2006; Raab and Milward 2003), including criminal enterprises (e.g., Malm and Bichler 2011; Malm, Kinney and Pollard 2008; Morselli 2010; Morselli and Giguere 2006), terror cells (Krebs 2002; Koschade 2006) and even corrupt police (Lauchs et al. 2011). Dupont (2006) is one of the few to use social network analysis in an attempt to map security networks.

As a form of organisation, a 'network' refers to a specific form of governance in contrast to the ideal-types of hierarchies and markets, and a form which has a number of advantages over these other forms (Powell 1990). Hierarchies are the more traditional mode of organising; they are differentiated horizontally through divisions between units and vertically through levels of authority, and are controlled through administrative means. Markets involve no consciously designed organisational structure as such, with the logic being that activities are loosely coordinated through price and contractual arrangements, with the law an instrument for resolving disputes between parties. Networks involve repetitive exchanges between a set

of autonomous but interdependent organisations to achieve particular objectives. Networks balance the ‘reliability’ of hierarchies with the ‘flexibility’ of markets, making them a more efficient way for organisations to acquire resources and manage risks (Ebers 1997) and more effective means of managing complex problems requiring coordination between organisations (O’Toole 1997). A networked organisational structure displays both ‘structural’ properties, involving the design, size and level of goal-consensus, and ‘relational’ properties concerning the formal and informal relationships between network members (Provan and Kenis 2008). Where the network is designed as a means of providing inter-agency coordination—or what network analysts call ‘goal-directed’ networks (Kilduff and Tsai 2003)—most tend to focus on the ‘formal’ rather than ‘informal’ relationships. However, the management literature points out that these informal ‘social networks’ are often crucial for ‘understanding how work really gets done’ (see Cross and Parker 2004).

‘Security networks’ need to be viewed as forms of organising (Whelan 2012) in order to understand how security agencies ‘work together’ to achieve their own goals as well as a collective or shared goal (see Provan and Kenis 2008). Dupont (2004) distinguishes between four ideal-types of security networks: local, international, institutional and virtual. While local and international networks differ in terms of their geographical parameters and points of focus, institutional and virtual networks are particularly relevant to sports mega events. Institutional security networks are platforms for inter-agency coordination (Brodeur and Dupont 2008). These networks may include local, national and international actors or agents and, in the context of sports events, public and private actors (Palmer and Whelan 2007). Institutional networks are likely to be located in a particular space, such as task forces, fusion centres and interdepartmental committees, the surveillance functions of which have received considerable attention (e.g., Monaghan and Walby 2012; Monahan 2010). Many examples of such networks are briefly provided in the London 2012 *Security Strategy*, including the National Olympic Coordination Centre, which was a multi-agency centre comprising links to key agencies headed by the National Olympic Security Coordinator, and was supported by several smaller and more specialised Strategic Coordination Centres (Home Office 2011b). However, institutional networks at sports mega events are likely to operate very differently to other more enduring institutional networks, particularly in terms of culture and trust, given they are temporary in nature.

Virtual networks provide the technical infrastructure enabling the communication and exchange of data and information between security agencies or agents (Dupont 2004). They might also apply to the surveillance systems collecting and managing data on individuals and relaying that data to various security agents (Monahan 2010). However, when security networks are viewed as a principle of organising, institutional and virtual or technological networks should be considered components of the broader security networks (Whelan 2011). For example, in the case of London 2012, the National Olympic Coordination Centre had access to video surveillance systems and the operational capacity to control how that surveillance data was used. Therefore, technological systems, including those designed to communicate between security agents or for the purposes of surveillance, involve broader complexities that can only be addressed when these issues are examined as part of the overall matrix of security initiatives that takes place in and through networks.

Designing a Framework for Research and Analysis

This paper now puts forward a framework for analysing networks, applying equally to those networks involved exclusively in surveillance or security activities, as well as those practicing both. It should be clear that surveillance practices occur in larger networks involving complex ‘structural’ and ‘relational’ dynamics. For example, video surveillance systems are not simply positioned in particular places but are linked to and monitored by a select group of agencies, which then may or may not communicate the content of this surveillance to other agencies. Security, as indicated earlier, is also highly dependent on the performance of these networks given they are central to inter-agency communication and coordination. Building on the standard structural and relational properties of networks, three additional foci of analysis

are also crucial. These are ‘cultural’, ‘policy’ and ‘technological’ dimensions, which intertwine with structural and relational factors to cover both the formal and informal aspects of networks. As such, these properties are interdependent and raise important questions about how agencies work together at sports mega events.

Network *structure* refers to the ‘design’ of a network, involving questions around the inclusion or exclusion of actors and related issues associated with coordination and governance. If the network does not comprise the required actors then it is unlikely to be effective in promoting meaningful inter-agency communication. At the same time, there is an optimum size to a network. The larger the network, the more difficult it is to manage. The internal coordination of network activities can be attempted in different ways (Kenis and Provan 2009). For example, Provan and Kenis (2008) distinguish between ‘brokered’ and ‘shared’ network governance. Brokered network governance refers to the use of a central or ‘hub’ design in which activities are controlled by a ‘lead organisation’. Shared network governance refers to a decentralised or ‘all-channel’ design in which all members are relatively equal. Large security networks are likely to have elements of both designs, whereby some ‘clusters’ within the network will be more concentrated than others, and those clusters may be connected through both direct or indirect ties (Dupont 2006). The essential point is that some security networks can involve brokers or lead organisations, which specifically coordinate the activities of network members, and other networks may have little or no internal coordination. The design of these networks is also likely to change in different operational contexts. For example, when responding to security problems increased coordination is often required. In the context of sporting mega events, the sheer size of the ‘security assemblage’ suggests that the challenges involved in designing networks, encompassing local, national and international actors, are immense. While some have commented on the operational plans for how this has been done, such as with London 2012 (Weston 2011), there is limited analysis on the importance of network design. This gap in contemporary research is crucial to surveillance and security scholars alike, as the design of networks is central to understanding the structural processes of inter-agency communication and coordination.

Network *culture* examines both cultures *within* networks and the culture *of* networks. Schein (2004: 17) suggests that culture is to a *group* what personality is to an *individual*: the beliefs, values and attitudes which form over the course of a group’s history and influence how it thinks and acts in relation to specific problems. A ‘group’ can be defined as ‘as any social unit that has some kind of shared history’ (Schein 2004: 11). It can refer to networks (‘network culture’), organisations (‘organisational culture’) and units or divisions within organisations (‘organisational sub-cultures’). The strength of any particular group’s culture will depend on many factors, including the length of its history, the stability of its membership and the types of experiences its members have shared. Culture has a profound impact on the extent to which communication and collaboration takes place in networks. This is particularly true of surveillance and security networks, where cultural barriers between police, security and intelligence agencies, and between public and private sector agencies, can result in serious problems that can undermine security (Boyle 2012; Manning 2006; Warren 2002; Whelan 2012). For example, Ryan (2003) describes culture as one of the key sources of inter-agency rivalry. The cultures of security networks themselves, and the cultural differences between network members, are research questions likely to significantly advance our knowledge of the issues associated with surveillance and security governance at sports mega events.

Policy concerns the formal procedures that aim to prescribe courses of action to actors in networks (Kenis and Provan 2006). Policy applies to any number of network activities and has important bearing on the processes of inter-agency communication, including helping with delineating roles and responsibilities of actors that sometimes overlap and at other times conflict. The most obvious example concerning networks in the field of national security is the requirements placed on the protection of security-classified information, including the ‘need-to-know’ principle (see de Bruijn 2006). Any policy framework setting out the types of information to be shared with certain agencies requires consideration of the multiple security classifications and levels of access to that information. Those at the ‘core’ of the network usually

control information centrally and distribute elements out to the ‘periphery’. The 9/11 Commission Report identified a problematic tension between ‘information protection’ and ‘information sharing’ (National Commission on Terrorist Attacks Upon the United States 2004: 417), arguing that agencies must adopt a ‘need-to-share’ information culture rather than retain their default position of needing to protect information to ensure appropriate levels of inter-agency communication. A tension is also evident here because adopting a policy that promotes the widespread sharing of information can be enormously problematic, with networks likely to collapse under the weight of ‘information overload’ (Brodeur and Dupont 2008). Crucial surveillance and security questions have long included the types of information that are gathered and shared, and the potential implications of such practices for individual privacy (e.g., Monahan 2010). However, precisely how surveillance and security information should be communicated remains a question that needs to be answered, particularly in relation to what level of information sharing is necessary to promote security.

Network *technology* relates to the ‘infrastructure’ that enables the processing of information between members of security networks. The most important aspects of technological infrastructure relate to the ways in which information and communication systems are *designed* in the context of a network’s structure, and how they are to be *used* by network members. In security-sensitive fields, an overriding consideration involves balancing ‘information protection’ with ‘information sharing’ (Desouza 2009). The design of surveillance, information and communication systems has traditionally been problematic for security networks (Whelan 2012). Manning (2006) is among the few to address this issue in relation to sports mega events. A common problem is the lack of interoperable systems, which compromises network design and the capacity of technological systems to process large volumes of information. While security technologies are arguably the primary focus of research into these dynamics and problems of surveillance at sports mega events (e.g., Bennett and Haggerty 2011; Coaffee et al. 2011; Fussey et al. 2011; Fussey and Coaffee 2012a), the overwhelming focus on these issues as contentious practices overlooks the necessity for sophisticated information and communication technologies to process and distribute information amongst diverse local, national and international security agencies. It is necessary to understand and recognise these broader purposes of surveillance and the extent to which technological systems can and do improve security at large-scale sports mega events.

Network *relationships* encompass both ‘micro’ interpersonal relationships and ‘macro’ relationships between work units and organisations (see Brass, Galaskiewicz, Greve and Tsai 2004; Kilduff and Krackhardt 2008). ‘Social networks’ involve *informal* relationships while ‘organisational networks’ are commonly based on *formal* relationships between agencies. Both types of relationships require some level of ‘trust’ (see Rousseau, Sitkin, Burt and Camerer 1998: 395), with social networks based on ‘interpersonal’ trust while more complex and structured relationships involve ‘inter-organisational’ trust. Generally speaking, security networks at monolithic but temporary sports mega events are likely to be characterised by ‘swift trust’ (Meyerson, Weick and Kramer 1996), in contrast to traditional forms of ‘relational’ trust that develop over long periods of time. However, the precise dynamics of relationships and trust are likely to vary considerably amongst those at the ‘core’ of the network, who have typically been working together in the planning of the event for some time (Boyle and Haggerty 2012; Manning 2006), and those at the ‘periphery’, who progressively enter the security network leading up to the event. Trust also shapes the optimum size of a network. For example, as the level of trust increases, the need for networks to be internally controlled through formal surveillance and other mechanisms decreases. Trust moderates the effects of networks in complex ways, including how information is shared and with whom it is shared, which we have barely begun to examine in the context of sports mega events.

Conclusion

Sports mega events have attracted a considerable amount of attention in recent years from a range of perspectives. Events such as the Olympic Games, FIFA World Cups and Commonwealth Games are key

sites where surveillance and security intersect in complex ways. While there is no doubt that surveillance and security are and should remain discrete concepts (Lyon and Murakami Wood 2012), surveillance is a key method of promoting security at sports mega events. Most literature to date has focused on the questionable ways that surveillance technologies are introduced and deployed at sports mega events, particularly in light of their post event ‘security legacies’ (e.g., Bennett and Haggerty 2011; Coaffee et al. 2011; Fussey et al. 2011; Fussey and Coaffee 2012b). This paper calls attention to some other important surveillance and security questions. For example, rather than focus on how security technologies are directed towards monitoring and controlling the behaviour of sports spectators, this article focuses on how surveillance data and security technologies are used ‘behind the scenes’. This perspective focuses on surveillance and security practices within and between the agents involved in providing security rather than the potential targets of the security spectacle.

The practices of surveillance and security need to be understood in the broader context of networks. Surveillance technologies, for example, are a means by which data is collected and organised for a particular purpose. When that purpose is security, as is often (but not always) the case, the function of that data can only be properly understood in relation to various networks of security governance. The dynamics of these security networks at sports mega events have so far received limited scholarly attention. Other than the prevailing focus on surveillance technologies, scholars have tended to address security infrastructures in relation to urban design as well as other important questions about how security risks are defined, identified and managed (e.g., Fussey and Coaffee 2012a; Giulianotti and Klauser 2010; Richards et al. 2011). A network perspective recognises the broader complexity and interrelationship between surveillance and security practices, by focusing on how agencies communicate, coordinate and collaborate and otherwise ‘work together’ (Whelan *forthcoming*). The framework provided here involves examining security networks across five levels of analysis: structural, cultural, policy, technological and relational. Each level involves important but interdependent sets of questions associated with the processes of surveillance and mega event security. The structure of networks and the relationships between their members has different implications for those organising distinct sports mega events. In addition, critical cultural differences between surveillance and security agents and agencies, as well as the policies designed to regulate the terms of information exchange and technological practices enabling data exchange, are particularly important to agents practicing surveillance and security. More particularly, given the enormous complexity of the security assemblage, these questions are directly relevant to the organisation of surveillance and security, and future research into the interplay between these processes at sports mega events.

References

- Bennett, C. and K.D. Haggerty. 2011. Introduction to Security Games: Surveillance and Control at Mega-Events. In: *Security Games: Surveillance and Control at Mega-Events*, eds C. Bennett and K.D. Haggerty, 1-19. Hoboken: Routledge.
- Bennett, C. and K.D. Haggerty, eds. 2011. *Security Games: Surveillance and Control at Mega-Events*. Hoboken: Routledge.
- Borgatti, S. and P. Foster. 2003. The Network Paradigm in Organizational Research: A Review and Typology. *Journal of Management* 29(6): 991-1013.
- Boyle, P.J. 2011. Knowledge Networks: Mega-Events and Security Expertise. In: *Security Games: Surveillance and Control at Mega-Events*, eds C. Bennett and K.D. Haggerty, 169-184. Hoboken: Routledge.
- Boyle, P.J. 2012. Risk, Resiliency, and Urban Governance: The Case of the 2010 Winter Olympics. *Canadian Review of Sociology* 49(4): 350-69.
- Boyle, P.J. and K.D. Haggerty. 2009. Spectacular Security: Mega-Events and the Security Complex. *International Political Sociology* 3(3): 57-74.
- Boyle, P.J. and K.D. Haggerty. 2012. Planning for the worst: Risk, uncertainty and the Olympic Games. *The British Journal of Sociology* 63(2): 241-59.
- Brass, D., J. Galaskiewicz, H. Greve and W. Tsai. 2004. Taking Stock of Networks and Organizations: A Multilevel Perspective. *Academy of Management Journal* 47(6): 795-817.
- Brodeur, J.-P. and B. Dupont. 2008. Introductory Essay: The Role of Knowledge and Networks in Policing. In: *The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions*, ed. T. Williamson, 9-36. West Sussex: John Wiley & Sons.
- Buzan, B., O. Waever and J. Wilde. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner.

- Coaffee, J. and P. Fussey. 2010. Olympic Security. In: *Olympic Cities: City Agendas, Planning, and the World's Games, 1986-2012*, eds J. Gold and Margaret Gold, 167-79. Hoboken: Routledge.
- Coaffee, J., P. Fussey and C. Moore. 2011. Laminated Security for London 2012: Enhancing Security Infrastructures to Defend Mega Sporting Events. *Urban Studies* 48(15): 3311-27.
- Cross, R. and A. Parker. 2004. *The Hidden Power of Social Networks: Understanding How Work Really Gets Done in Organizations*. Boston, MA: Harvard Business School Press.
- de Bruijn, H. 2006. One Fight, One Team: The 9/11 Commission Report on Intelligence, Fragmentation and Information. *Public Administration* 84(2): 267-87.
- Desouza, K. 2009. Information and Knowledge Management in Public Sector Networks: The Case of the US Intelligence Community. *International Journal of Public Administration* 32(14): 1219-67.
- Dupont, B. 2004. Security in the Age of Networks. *Policing & 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(2): 165-84.
- Ebers, M. 1997. Explaining Inter-Organizational Network Formation. In: *The Formation of Inter-Organizational Networks*, ed. M. Ebers, 3-40. Oxford: Oxford University Press.
- Fussey, P. 2011. Terrorist threats to the Olympics, 1972-2016. In: *Terrorism and the Olympics: Major event security and lessons for the future*, eds A. Richards, P. Fussey and A. Silke, 239-43. London: Routledge.
- Fussey, P. and J. Coaffee 2012a. Balancing local and global security leitmotifs: Counter-terrorism and the spectacle of sporting mega-events. *International Review for the Sociology of Sport* 47(3): 268-85.
- Fussey, P. and J. Coaffee. 2012b. Olympic rings of steel: Constructing security for 2012 and beyond. In: *Security Games: Surveillance and Control at Mega-Events*, eds C. Bennett and K.D. Haggerty, 36-54. Hoboken: Routledge.
- Fussey, P., J. Coaffee, G. Armstrong and D. Hobbs. 2011. *Securing and Sustaining the Olympic City: Reconfiguring London for 2012 and Beyond*. Aldershot: Ashgate.
- Fussey, P., J. Coaffee, G. Armstrong and D. Hobbs. 2012. The regeneration games: Purity and security in the Olympic city. *British Journal of Sociology* 63(2): 260-84.
- Gill, M. 2006. Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001. *Policing & Society* 16(1): 27-49.
- Giulianotti, R. and S. Brownell. 2012. Olympic and world sport: Making transnational society. *British Journal of Sociology* 63(2): 199-215.
- Giulianotti, R. and F. Klauser 2010. Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda. *Journal of Sport and Social Issues* 34(1): 48-60.
- Giulianotti, R. and F. Klauser. 2011. Introduction: Security and Surveillance at Sport Mega Events. *Urban Studies* 48(15): 3157-68.
- Giulianotti, R. and F. Klauser. 2012. Sport mega-events and 'terrorism': A critical analysis. *International Review for the Sociology of Sport* 47(3): 307-23.
- Home Office. 2011a. *CONTEST*, UK Government, London (accessed 25-June-2012) <<http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat/>>
- Home Office. 2011b. *London 2012 Olympic and Paralympic Safety and Security Strategy*, UK Government, London (accessed 25-June-2012) <<http://www.homeoffice.gov.uk/counter-terrorism/2012-olympic-games/>>
- Hopkins, N. 2012. G4S Olympic security recruitment 'totally chaotic', *The Guardian*, London. <<http://www.guardian.co.uk/sport/2012/jul/12/g4s-olympic-security-recruitment-chaotic>>
- Hopkins, N. and R. Booth. 2012. Olympic security chaos: Depth of G4S security crisis revealed, *The Guardian*, London. <<http://www.guardian.co.uk/sport/2012/jul/12/london-2012-g4s-security-crisis>>
- Jennings, W. 2011. Governing the Games in an age of uncertainty: The Olympics and organisational responses to risk. In: *Terrorism and the Olympics: Major event security and lessons for the future*, eds A. Richards, P. Fussey and A. Silke, 135-62. London: Routledge.
- Jennings, W. 2012. *Olympic Risks*. London: Palgrave.
- Kenis, P. and K. Provan. 2006. The Control of Public Networks. *International Public Management Journal* 9(3): 227-47.
- Kenis, P. and K. Provan. 2009. Towards an Exogenous Theory of Public Network Performance. *Public Administration* 87(3): 440-56.
- Kilduff, M. and D. Krackhardt. 2008. *Interpersonal Networks in Organizations: Cognition Personality, Dynamics, and Culture*. Cambridge: Cambridge University Press.
- Kilduff, M. and W. Tsai. 2003. *Social Networks and Organizations*. London: Sage Publications.
- Klerks, P. 1999. The network paradigm applied to criminal organisations: Theoretical nitpicking or relevant doctrine for investigators? Recent developments in the Netherlands. *Connections* 24(3): 53-65.
- Koschade, S. 2006. A social network analysis of Jemaah Islamiyah: The applications to counterterrorism and intelligence. *Studies in Conflict & Terrorism* 29(6): 559-575.
- Krebs, V. 2002. Mapping networks of terrorist cells. *Connections* 24(3): 43-52.
- Lauchs, M., R. Keast and N. Yousefpour. 2011. Corrupt police networks: Uncovering hidden relationship patterns, functions and roles. *Policing and Society* 21(1): 110-27.
- Lenskyj, H. 2002. *The Best Olympics Ever? The Social Impacts of Sydney 2000*. Albany: Suny Press.

- Lippert, R. and D. O'Connor. 2006. Security Intelligence Networks and the Transformation of Contract Private Security. *Policing and Society* 16(1): 50-66.
- Loader, I. 2002. Policing, securitization and democratization in Europe. *Criminology & Criminal Justice* 2(2): 125-53.
- Lyon, D. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.
- Lyon, D., K.D. Haggerty and K.S. Ball. 2012. Introducing Surveillance Studies. In: *Routledge Handbook of Surveillance Studies*, eds K.S. Ball, K.D. Haggerty and D. Lyon, 1-11. London: Routledge.
- Lyon, D. and D. Murakami Wood. 2012. Security, Surveillance, and Sociological Analysis. *Canadian Review of Sociology* 49(4): 317-27.
- MacDonald, M. and D. Hunter. 2013. The discourse of Olympic security: London 2012. *Discourse and Society* 24(1): 66-88.
- Malm, A. and G. Bichler. 2011. Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. *Journal of Research in Crime and Delinquency* 48(2): 271-297.
- Malm, A., B. Kinney and N. Pollard. 2008. Social network and distance correlates of criminal associates involved in illicit drug production. *Security Journal* 21: 77-94.
- Manning, P. 2006. Two case studies of American anti-terrorism. In: *Democracy, Society and the Governance of Security*, eds J. Wood and B. Dupont, 52-85. Cambridge: Cambridge University Press.
- Meyerson, D., K. Weick and R. Kramer. 1996. Swift Trust and Temporary Groups. In: *Trust in Organizations*, eds R. Kramer and T. Tyler, 166-95. London: Sage Publications.
- Milward, B.H. and J. Raab. 2006. Dark networks as organizational problems: Elements of a theory. *International Public Management Journal* 9(3): 333-360.
- Monaghan, J. and K. Walby. 2012. Making up 'Terror Identities': Security intelligence, Canada's Integrated Threat Assessment Centre and social movement suppression. *Policing & Society* 22(2): 133-151.
- Monahan, T. 2010. *Surveillance in the Time of Insecurity*. New Brunswick, NJ: Rutgers University Press.
- Morselli, C. 2010. Assessing vulnerable and strategic positions in a criminal network. *Journal of Contemporary Criminal Justice* 26: 382-392.
- Morselli, C. and C. Giguere. 2006. Legitimate strengths in criminal networks. *Crime, Law and Social Change* 45(3): 185-200.
- National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report*. Washington: US Government.
- O'Toole, L. 1997. Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration. *Public Administration Review* 57(1): 45-52.
- Palmer, D. and C. Whelan. 2006. Counter-Terrorism across the Policing Continuum. *Police Practice and Research* 7(5): 449-465.
- Palmer, D. and C. Whelan. 2007. Policing in the 'Communal Spaces' of Major Event Venues. *Police Practice and Research* 8(5): 401-408.
- Palmer, D. and C. Whelan. 2014. Policing and Networks in the Field of Counterterrorism. In: *Examining Political Violence: Studies of Terrorism, Counterterrorism, and Internal War*, eds D. Lowe, A. Turk, and D.K. Das, 145-166. Boca Raton: CRC Press.
- Porter, K. and W. Powell. 2006. Networks and Organizations. In: *The SAGE Handbook of Organization Studies*, 2nd Edition. eds S. Clegg, C. Hardy, T. Lawrence and W. Nord, 776-99. London: Sage Publications.
- Powell, W. 1990. Neither Market nor Hierarchy: Network Forms of Organization. In: *Research in Organizational Behavior*, Volume 12, eds S. Barry and L. Cummings, 295-336. Greenwich: CT JAI Press.
- Provan, K., A. Fish and J. Sydow. 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 P. Kenis. 2008. Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of Public Administration Research and Theory* 18(2): 229-52.
- Richards, A., P. Fussey and A. Silke, eds. 2011. *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge.
- Raab, J. and P. Kenis. 2009. Heading Toward a Society of Networks: Empirical Developments and Theoretical Challenges. *Journal of Management Inquiry* 18(3): 198-210.
- Raab, J. and B. Milward. 2003. Dark networks as problems. *Journal of Public Administration Research* 13(4): 413-439.
- Rousseau, D., S. Sitkin, R. Burt and C. Camerer. 1998. Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review* 22(3): 393-404.
- Ryan, P. 2003. Olympic Security: The Relevance to Homeland Security. In: *The 2002 Olympic Winter Games: Security Lessons Applied to Homeland Security*, ed. The Oquirrh Institute, 23-7. Salt Lake City: The Oquirrh Institute.
- Schein, E. 2004. *Organizational Culture and Leadership*. San Francisco, CA: Jossey-Bass.
- Sparrow, M. 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13(3): 251-274.
- Taylor, T. and K. Toohey. 2011. Ensuring Safety at Australian Sport Event Precincts: Creating Securitised, Sanitised and Stifling Spaces? *Urban Studies* 48(15): 3259-3275.
- Thompson, A. ed. 1996. *Terrorism and the 2000 Olympics*. Canberra: Australian Defence Studies Centre.
- Toohey, K. and T. Taylor. 2012. Surveillance and securitization: A forgotten Sydney Olympic legacy. *International Review for the Sociology of Sport* 47(3): 324-37.
- Valverde, M. 2011. Questions of security: A framework for research. *Theoretical Criminology* 15(1): 3-22.

- Waever, Ole. 1995. Securitization and Desecuritization. In: *On Security*, ed. R. Lipschultz, 46-86. New York: Columbia University Press.
- Warren, Ian. 2002. Governance, Protest and Sport: An Australian Perspective. *Entertainment Law* 1(1): 67-94.
- Weston, Keith. 2011. The challenge of inter-agency coordination. In: *Terrorism and the Olympics: Major event security and lessons for the future*, eds A. Richards, P. Fussey and A. Silke, 180-207. London: Routledge.
- Whelan, C. 2011. Network Dynamics and Network Effectiveness: A Methodological Framework of Public Sector Networks in the Field of National Security. *Australian Journal of Public Administration* 70(3): 275-286.
- Whelan, C. 2012. *Networks and National Security: Dynamics, Effectiveness and Organisation*. Aldershot: Ashgate.
- Whelan, C. *forthcoming*. Managing Dynamic Security Networks: Toward the Strategic Managing of Cooperation, Coordination and Collaboration. *Security Journal*.
- Yu, Y., F. Klauser and G. Chan. 2009. Governing Security at the 2008 Beijing Olympics. *The International Journal of the History of Sport* 26(3): 390-405.
- Zedner, L. 2009. *Security*. London: Routledge.