CHAPTER 19

THE SECURITY AGENCIES' PERSPECTIVE

Tracy Taylor (University of Technology, Sydney) and Kristine Toohey (Griffith University) (Australia)

INTRODUCTION

This chapter provides an overview of the context of sport event security and of the various types of security agencies (local, national, international, public, and private organisations), and other related stakeholders involved in the planning and hosting of sport events. Following this overview, research associated with risk, sport event security and safety is presented. The chapter concludes by providing suggestions for further reading and future research directions.

The organisation and delivery of sport events now requires an increasingly systematic approach to governance, including planning and managing for every kind of possible risk. This process of risk management incorporates the use of security measures to ensure that event venues, spectators, athletes and officials are kept safe. In this chapter, security is defined as a range of measures adopted by event stakeholders to maintain order, enforce relevant legislation, prevent and detect crime, and ensure a feeling of safety. The definition of risk management used is, "risk management is a proactive process that involves assessing all possible risks to the events and its stakeholders by strategically anticipating, preventing, minimizing, and planning responses to mitigate those identified risks" (Leopkey and Parent 2009: 187).

Security at sports events is affected by a range of factors, from local contextual and historical aspects (e.g. spectator related tensions) to larger geopolitical influences (e.g. political or religious motivation). The reaction to the rising awareness and categorisation of such risks, either real or perceived, has been an increase in strengthening events' protective infrastructure, especially since 9/11 (Boyle and Haggerty 2011). Evidence of the increases have been seen at a range of large and smaller sport events, such as the Olympic Games; Union of European Football Associations (UEFA) and The Fédération Internationale de Football Association (FIFA) events, especially those involving countries with terrorist connections; cricket games involving Pakistan; and domestic events such as United States (US) college football games, to name just a few.

This contemporary focus on public safety, security and risk mitigation has contributed to a range of improvements in event technology, staff training, and operational procedures and practices. Correspondingly, the resources allocated to security at sports events have also significantly escalated. Security expenditure was $180 million for the Sydney 2000 Olympic Games, while security costs topped an estimated $1.9 billion at the London 2012 Olympic Games.

Safety and security issues are of a primary concern for a range of event stakeholders, specifically key decision-makers, governments, media and the public. These security stakeholders have different control powers, interests, needs and agendas, although each anticipates specific benefits for their contribution to the organisation and staging of sport events (Parent 2008).

Terrorism (e.g. the 2013 Boston Marathon, the 1996 Atlanta Centennial Olympic Park bombing, and the Olympic Games terrorist attack in Munich 1972) is generally regarded as the most serious security issue, especially from the perspective of the Western media (Atkinson and Young 2012). However, such acts of terrorism have been infrequent, when compared to other security issues. Essentially, the main security risks differ, depending on the size, type and context of the sport event, however, generally the majority of risks are associated with illegal crowd behaviour (e.g. public intoxication, spectator aggression), local crime (e.g. ticket scalping), political activism (e.g., 'anti-event' protests, strikes) and terrorism (e.g. bombs or shootings).

Sports event stakeholders have developed sophisticated bid documentation and operation manuals to counteract these risks and dictate how security is to be managed. For example, the International Olympic Committee (IOC) has introduced a *Candidature Procedure and Questionnaire*. Essentially, this document functions as an evaluation process by which the IOC's Evaluation Commission assesses each applicant city on a number of decision-making criteria, each of which is essentially an implicit indicator of risk. Additionally, often in agreeing to host events, local, regional and/or federal governments have been required to introduce specific event related legislation, by-laws and other legal mechanisms to protect venues and limit risk. However, many of these legal arrangements have been questioned in terms of impingements of citizen/human rights (Taylor and Toohey 2011).

The implementation of policies and practices in relation to sport event security typically involves an exercise of power by one or more of the event stakeholders. While the mechanisms developed to cope with perceived event security risks have led to the development of greater community resilience (Boyle and Haggerty 2009), it has also been suggested that sport events have been used as a 'laboratory' for introducing new security systems, allowing heightened securitisation processes to expand beyond the boundaries of the event for which they were originally conceived (Giulianotti and Klauser 2010). Additionally, Eick (2011a) has questioned the use of power, implemented under the guise of risk management, by event owners/organisers, which can control and influence the host city's security and surveillance strategies, as well as its urban design.

OVERVIEW OF THE STAKEHOLDER GROUP

Sport event security especially, but not exclusively, at the sport mega event (SME) level, has become increasingly multifaceted, multi-layered, pre-emptive, pervasive, technologically dependent, politically responsive, complicated, commoditised and costly. Such demands can strain the resources of event organisers. These security transformations have also impacted all levels of sports events and have meant that the number, variety and power of sport event stakeholders involved in security aspects have increased concomitantly.

Sport event security stakeholders now come from the public, private and voluntary sectors at local, national and international levels. These stakeholders can include international and national intelligence services, homeland security departments, event-dedicated intelligence agencies, immigration agencies, police forces, military personnel and security contractors hired by the event. Understandably, this mixture can result in vastly different and even

conflicting interests, approaches and agendas with various other event stakeholders, including the event organisers.

Generally, the security services and police tend to focus their attention on categories such as threats from crime, disorder and domestic or international terrorists, whereas the event organising committees tend to be more interested in a wider portfolio of security issues affecting the organisation and operation of the event, such as hooliganism. As a result, from an operational perspective:

> The process of coordination and management of SMEs engages multiple and heterogeneous stakeholders coming from the private and public spheres. As a result these mechanisms cannot be conceptualised, exclusively, according to a vertical, hierarchical, linear and state-centred vision. On the contrary, they should be comprehended following a more horizontal and fluid configuration, linking together private and public forces and overlapping the clear distinction between public and private spheres... they should not be restricted to a territorial conception... security consists of dynamic, extensive operations... developed through an inter-institutional, supranational labyrinth of different networks within governments, outside governments and within the grey areas between, beyond the national territory transcending the borders of the host country (Mastrogiannakis and Dorville 2013: 135).

Essentially, a sport event security stakeholder is any organisation or person who has something to gain or lose through a security based-relationship with the event. Thus, sports events need to adapt to and influence the changing expectations, motivations and perceptions of their stakeholders.

Stakeholders have legitimate interests in an organisation or event; and the interests of all stakeholders are of inherent value to the organisation or event. The application of stakeholder theory to sport organisations has revealed that there can be complex networks of contiguous stakeholders and an even more convoluted framework of those whose associations are more distant but nevertheless need to be considered (Hoye and Cuskelly 2007). All sports events, no matter how big or small, can be advantaged or constrained by their stakeholders' varied agendas, including those agendas relate specifically to security.

Eisenhauser (2013) suggested four global influences on current security management processes at sports events: a general increase in commercialisation and commoditisation; globalisation; technologisation; and mediatisation. The current crucial place of security as an integral part of the planning and staging sport events both reflects and influences the increasing importance, especially in Western institutions and societies, of the implementation of formal risk management controls, practices and requirements, as well as the ongoing fear of major security problems, such as terrorism.

While risk management practice itself is becoming more rigid and isomorphic (cultural and geopolitical differences not withstanding), it still requires choices of: 'which risks to discount, which to monitor, and which risks to mitigate and protect against' (Jennings and Lodge 2009: 8). While 'safety and security have always been a key function of stadium and arena management, with venue managers needing to keep their venues safe and secure within a broad risk management perspective' (Sweaney 2005: 22), since the 11 September 2001 (9/11) attacks, the threat of terrorism has brought risk and security management to the forefront of sport event planning, especially for mega and major events.

The response of sport stakeholders has resulted in increased security measures (for both safety and insurance requirements), not only in the event venues, but also within the surrounding event precinct and even host cities. This has at times been enacted through a technologically-driven social control agenda that has been criticised for the potential to subjugate individuals' rights (Taylor and Toohey, 2011). Such an approach becomes increasingly problematic when these measures are aimed at particular social groups in an effort to sanitise an event's space and can inhibit spectator enjoyment for the majority. For example, previously acceptable and seemingly innocent practices, such as beating drums, waving flags, and even the "Mexican Wave" have been forbidden in some venues, under the guise of providing a safe spectator environment.

In addition to these changes, Clavel (2013: 209) cautions that preventative and intrusive high tech surveillance and securitisation is dominating contemporary sport event security discourse and practice. Spaaij (2013) suggests that this panopticised approach is a result of the growing emphasis on authorities' use of predictive, anticipatory and preventative action, to control all possible sources of danger before they might occur. Further, he suggests that this pre-emptive discourse of risk management means that any level of risk, however slight, is deemed unacceptable and is monitored. This has meant there has been increasing cooperation around sports events between security agencies and nations, which may have not collaborated previously or even been opponents (Clavel 2013).

Thus, sport event security has been affected by events and stakeholders outside of sport, resulting in increased surveillance and other deterrent measures. However, sports events have

not only been a passive recipient in this connection. Clavel (2013) notes that SMEs have affected the upwards re-calibration of everyday security processesand have become laboratories for the testing security measures, especially those using the latest technologies. Additionally, the introduction of ongoing and improved international security collaborations between the events' security stakeholders, including governments nationally and internationally, has improved.

The scale, location, and format of a sports event influences its stakeholders' approach to risk and security. For example, multi-sport events, such as the Olympic Games, are mostly concentrated in precincts in a single city or region, thus concentrating risk to a relatively condensed geographical area. However, football, rugby, and cricket world cups are usually spread over a larger area and may even be co-hosted by more than one country. They may also occur over a significantly longer period of time, leading to more potential trouble spots, however this also means a corresponding diffusion of risks (Jennings and Lodge 2009).

Additionally, the types of security threats and thus stakeholder responses differ between different forms of sports events, especially SMEs. While the Olympic Games have been associated with geopolitical conflicts (such as between North and South Korea in 1988) and/or terrorism (Munich 1972),

> international football tournaments tend to be associated with pubic disorder, violence and organised hooliganism; with large crowds of national (and sometimes local) supporters who gather for specific matches during concentrated periods of competition. This contrasts with the Olympics where... spectators... tend to comprise diverse/transnational audiences that do not divide their support across different teams that symbolise historical lines of national conflict.

> Olympics, Football World Cups and European Championships therefore each encounter the problem of creating a platform for racist, nationalist and anti-capitalist demonstrations, and associated disorder or rioting- but the ways in which they are likely to be realised varies quite significantly (Jennings and Lodge 2009: 10).

In terms of the organisational and strategic focus of security stakeholders, generally security services and police focus their attention on categories such as threats of crime, disorder, and domestic or international activists and terrorists. The presence of the military in sport events has increased in line with 'the war on terror'. For SMEs such as the Olympic Games or FIFA World Cup, the national government of the host city or country is required by the international body in charge of the event (i.e. IOC or FIFA) to ensure the safety of athletes and officials. Event organising committees tend to be interested in a wider portfolio of security issues affecting the day to day organisation and operations of the event. Thus, sport event organising committees usually do not control security but must somehow coordinate it.

Planning for sport event security "involves a strategic process of reviewing recent past events to identify potential threats" (Johnson 2006: 3), followed by the allocation of resources to prevent the same type of incidents. There is a great deal of homogeneity of security measures and responses. This standardised, mimetic approach is understandable as event security decisions

> are taken in a state of high uncertainty (and with high search costs for weighting information), therefore encouraging searches for options that are perceived to be legitimate and successful (mimetic source of isomorphism). Second, given the rise of risk management consultocracy over the past decade

> or so, we can also expect risk management tools to travel across domains, thereby performing what Di Maggio and Powell call, normative sources of isomorphism. Accordingly, we would expect the presence of a dominant or hegemonic discourse regarding appropriate tools of security risk management to lead to homogeneous application of risk management tools. Finally, a further source for institutional isomorphism is of a coercive nature, and is not difficult to find such sources that apply for the security risk management of major sport events, namely the 2004 EU Handbook on avoiding terrorist acts at major sporting events, as well as the 1985 European Convention on Spectator Violence at Sport Events, especially in football (Jennings and Lodge 2009: 4).

Similarly, there has been 'standardization in stadium designs and emphasis upon the importance of creating similar 'response environments' so that first responders in emergency situations do not require extensive familiarization with peculiarities of each location, such as in relation to exit routes, evacuation plans and so forth' (Jennings and Lodge 2009: 13). While event organisers and venue managers support the evolution of stadia and event control in terms of comfort and safety; criticism has come from traditional sport event attendees, themselves important stakeholders, who question the lack of atmosphere associated with modern dedifferentiated stadia (Paramio, Babatunde, and Campos 2008).

However, not all academics and/or practitioners agree with this view that security is now standardised. For example, Spraaij (2013) argues the opposite and claims that the growing number and range of security stakeholders has in fact led to security decentralisation and/or functional differentiation and specialization leading to bespoke event safety measures.

In terms of security technology, closed circuit television (CCTV) is becoming increasingly ubiquitous for monitoring spectator behaviour both at sport event venues and in surrounding public places. The CCTV system may be equipped with recognition software. For example, biometric face recognition cameras were implemented at the 2006 World Cup in Germany. Also increasingly, the CCTV cameras remain after the event concludes, leading to increased and ongoing surveillance of the general public, and potentially intruding on individuals' civil liberties. Thus, temporary event security measures may become permanent as surveillance mechanisms are used for general public surveillance. This will be discussed in greater detail later in this chapter.

Intelligence and security data is increasingly being shared by event security stakeholders on a transnational basis for international events. For example, for the 2006 World Cup, Germany built on bilateral agreements it had in place with 36 other nations. These mechanisms had already been utilised in previous European football tournaments, as well as for the Athens 2004 Olympic Games (Jennings and Lodge 2009). Furthermore, existing international forces such as North Atlantic Treaty Organization (NATO) and Interpol (which signed an agreement on 9 May, 2010 to share data and cooperation) may be involved (Clavel 2013: 210). Additionally, specific international security agencies have been created for SMEs. For example, each Olympic Games 'since Atlanta 1996, has created an Olympic Intelligence Centre (OIC) to assimilate information and risk assessments for intelligence of Olympic interest through cooperation and information-sharing protocols involving over one hundred countries and international organisations' (Jennings and Lodge 2009: 11).

On a domestic basis this security cooperation also occurs. For the 2012 London Olympic Games,

> existing intelligence agencies (such as the Joint Intelligence Committee, MI5, MI6, [Government Communications Headquarters] GCHQ and the Defence Intelligence Staff) intersect with a number of Olympic specific coordinating organizations: in particular the Cabinet-level Olympic Security Committee and the Metropolitan Police's Olympic Security Directorate (OSD). An Intelligence Unit has been established within the OSD to gather and share information between security stakeholders for London 2012 (Jennings and Lodge 2009: 11).

While there is a legitimate and important place for risk management and technology in sport event management, organisers also need to understand the range of emotional responses to these solutions. As Durodie (2007) argues, too much reliance on technical solutions can actually heighten the sense of risk. He also notes that

> perceptions of risks are as important - if not more so - than the actuality of the risks we face, as perceptions often determine behaviour. Thus... irrespective of the basis for such fears in scientific fact, their effects are real in social consequence, leaving governments with little choice but to take such concerns on board and to regulate accordingly (Durodie 2007:76).

THE ROLE OF THE STAKEHOLDER

As previously discussed, hosting a sports event requires significant risk assessment, security investment and the projection of resilient security strategies. This investment is generally proportional to the scale of the event, with local community events at one end of the spectrum and the events that attract an international audience, either as spectators or via media

channels, at the other end. The many faceted community and commercial drivers that underpin sport events obviously impact on stakeholders' desire to maintain control over key security and surveillance activities.

Irrespective of event size or scope, nearly all post-9/11 security budgets have escalated in response to contemporary perceptions of threats of terrorism. Although there is a low risk of an actual terrorism incident occurring during an event, there appears to be heightened public demand for all possible contingencies to be covered. While tens of thousands of sports events run each year without incident, it only takes one high profile situation, such as the Boston Marathon bombings on 15 April 2013, which killed three people and injured 264 others, to increase public demand for 'better' security and safety. In carrying out an assessment of the risk of terrorism in the 2020 Olympic Games Applicant Cities, the 2020 Evaluation Commission noted, 'any city in the world can be subject to a terrorist attack either by local or international terrorist groups' (International Olympic Committee 2012b: 3).

Significant resources are invested in a range of security strategies for sport events. These may be activated by the event owner, host cities and/or nations. Security strategies in public spaces encompass an extensive range of public order, risk, safety and stakeholder brand protection and commercial interests associated with an event. As extracted below, the case of the 2010 FIFA World Cup (FWC), hosted by South Africa, is a demonstration of the scale of safety and security planning and the range of stakeholders required to host a modern large scale event.

The FIFA World Cup – South Africa 2010

South African Police Service had a budget of about R1.3 billion (equivalent to USD 146 million) to address safety and security at the FWC. This is similar to the 2000 Sydney Olympics budget (USD 179.6 million), but only about one-eighth of the security budget of the 2004 Athens Olympics and 2006 Turin Olympic Winter Games, and less than five per cent of the security expenses at the 2008 Beijing Olympics. Approximately R640 million was allocated for the deployment of 41,000–44,000 officers. Some R665 million was spent on procuring special security equipment, such as crowd management equipment and associated body armour.

The City of Cape Town safety and security plan alone accounted for an additional seven fire engines; seven law enforcement vehicles; seven traffic motorcycles; 124 fire fighters; 35 traffic officers; 21 disaster-management officers and 180 law-enforcement officers. More than 440 jobs were created and approximately 2,500 people were trained in crowd management and the overall safety and security plan involved 3,600 existing police officers throughout the Western Cape Province. Some 1,200 new South African Police Service members were trained in basic policing, firearm usage and first level crowd management.

There was a 24-hour Provincial Joint Operation Centres in each province where tournament matches were played. In the Western Cape, they were based at what was called the Police 'War Room', in Cape Town's CBD and coordinated with the Venue Operation Centres (VOC) and mobile command centres that were set up at the Green Point stadium and at each site along the event footprint across the province, including all public viewing area sites. The VOC had representatives from Law Enforcement, Emergency Services, South African Police

Services, South African Health Military Services, Traffic Services, Metro Police Services, Fire and Rescue, Disaster and Risk Management Services, Event Management, Event Security Services and other related agencies.

The Deputy National Police Commissioner remarked, 'a World Cup is a dream for every police chief – I can ask for anything, and I get it!'

(Extract from Eisenhauer 2013:145).

As can be ascertained from the FIFA World Cup example, event safety and security involves a complex array of stakeholders. With respect to the Olympic Games, Girginov and Gold (2013) reported that the London Organising Committee of the Olympic and Paralympic Games operations required interaction with over 150 different agencies, including all spatial domains of government, and national and international sponsors and partners. They also noted that 'LOCOG had virtually no pre-existing knowledge and expertise on which to draw in matters concerning security, transport, international relations, national coordination, emergency services and city logistics' (Girginov and Gold 2013: 17).

Table 1 outlines key event stakeholders and some of the more common security related interventions that they typically pursue. These stakeholders will also interact and respond to the local community, athletes, performers, event attendees and associated sport organisations that are involved with the event. The security related expectations of each stakeholder, and that of the event organiser toward each stakeholder, will vary depending on their relationship. Stakeholder expectations can be communicated through consultation, contracts, on-site inductions and performance monitoring, feedback and evaluation.

The key interventions identified in Table 1 are each overviewed below with examples of occurrences.

INSERT TABLE 1 ABOUT HERE

Legislation

It has become common practice, and indeed mandated by some event owners, for the hosts of international events, to introduce new legislation as part of the event agreement. Typically, these laws and regulations grant police increased powers of control over public spaces (Giulianotti and Klauser 2011), or the right to introduce what might be considered as intrusive surveillance mechanisms. There are many instances of security-related law reform and government intervention. For example, prior to the Athens Olympics, under international pressure, the Greek Parliament passed a new anti-terrorist law (2928/2002). Post 9/11, there has been a greater mass surveillance and maximum security presence, sanctioned by host city/country legislative changes. It has been suggested that governments are often manipulated into enacting event-specific legislation as a cost of doing business in exchange for hosting the event (Grady, McKelvey and Bernthal 2010).

Legislation may be specific to a single event. For example, in the lead up to the Sydney 2000 Olympic Games, the New South Wales Parliament passed three new pieces of legislation: the Homebush Bay Operations Act and Regulation 1999, the Security Industry (Olympic and Paralympic Games) Act 1999, and the Sydney Harbour Foreshore Authority Regulation 1999

("the Olympics Security Legislation"). The premise of this new legislation was to control behaviour within public spaces (Toohey and Taylor 2012). Broad powers were granted to police and other authorities to ensure public order was maintained by directing people to move on when behaviour was deemed to constitute obstruction, harassment or intimidation of others. The introduction of this legislation was met with some criticism due to the discretionary decision-making power given to the police to control public space and the disregard of civil liberties. Further, there has been much written about the temporary privatisation of public spaces to allow for more intensive surveillance by contracted security companies during events than would normally be allowed by police (See: Eick and Töpfer 2008; or Eick 2011a and 2011b for more detailed discussion).

In a study of the 2010 FIFA World Cup held in South Africa, Eisenhauer (2013) reported that the Planning Committee was required to incorporate certain legislation and regulation into their safety and security plans, including the 2010 FWC South Africa Special Measures Acts (no. 11 and 12. of 2006) and the 2010 FWC By-law(s). Similarly, in the candidature documentation for its 2020 Olympic Games bid, Istanbul confirmed that construction legislation had been modified to comply with high earthquake resilience standards, and a national budget of USD 40 billion will support the ‘Earthquake Resilience Plan’ which includes the retrofitting of sports venues (IOC 2012a: 29).

Legislative change is not only instigated by the hosting of mega-events, governments also enact new or amended legislation concerning domestic sports events. Hall (2010) noted the numerous legislation and security measures enacted by the British government to combat hooliganism, crowd control, and terrorism incidents. These included The Football Disorder

Act (1989); Football Spectators Act (1989); Football Offenses Act (1991); Football Act (1999); Football Disorder Act (2000); and Football Disorder Bill (2001). He suggested that these measures

> prohibited hooliganism, categorized the different offenses that a person would be charged with, covered both domestic and international terrorist threats to sport stadiums, and assured that individuals who were banned would be prevented from attending matches inside and outside of Britain (Hall 2010).

Interestingly quarantined to football, each football club must attain a stadium 'Safety Certificate' and designate a Safety Officer to assist facility management with safety strategies on match day and the recruitment and training of all stewards.

In their report on Olympic Games knowledge transfer, Girginov and Gold (2013) note that the London Organising Committee of the Olympic and Paralympic Games benefited significantly from a number of special conditions that were created specifically for the realisation of the Games. This included special legislation and security, and as suggested 'this unprecedented level of bracketing is afforded only to the Olympics, as a project of exceptional national and international significance' (Girginov and Gold 2013: 17).

Event related safety and security legislation may also be internally oriented. For example, in Australia, the Victorian Occupational Health and Safety Act 2004 (the OHS Act) stipulates that event organisers have a duty of care to provide a safe operational environment for employees. Under this legislation, event organisers must ensure so far as reasonably

practicable that: people are not exposed to risks arising from the operation; and any place where employees and self-employed persons work is safe (WorkSafe Victoria 2006).

Urban planning/development

The controlled or planned development of an area for large event hosting is another common safety and security related practice. The control elements may relate to the safeguarding of a range of stakeholder concerns and interests, including protecting local residents from crime and violence connected with the event, preventing spectator related disturbances, through to averting terrorism attacks. Common to this are associated government sanctioned urban development initiatives in and around event precincts (Haferburg 2011). Eick (2011a) has noted how urban renewal became a goal of the Olympics in the 2000s and, that FIFA has a similar stance on how facilities used in hosting the World Cup should be linked to strategies for urban regeneration.

In a study of three cities' sport event strategies, Misener and Mason (2009) explored the links between hosting sporting events and community development initiatives. In Edmonton (Canada), the sports events strategy was not seen to be directly tied to community development objectives. However, in Manchester (UK) and Melbourne (Australia), the use of events for development was linked to communities and community development goals. Examples were presented of symbolic attempts to foster community development around the sporting events' strategies.

Yu, Klauser and Chan (2009) noted that there are often wider social and political implications and complications connected with these event security-related developments; and Hall (2006) opined that SMEs can be used as a political instrument to conceive or legitimise urban development strategies. Notably, alongside the many positive initiatives and renewal projects associated with event driven urban planning and development, some projects have been shrouded in controversy. For example, the Indian city of Delhi hosted the 2010 Commonwealth Games as an opportunity to increase foreign investment levels and become a powerful world player. Delhi underwent significant urban and infrastructure development, including new sport stadiums, a new link road network and notably controversial beautification campaigns which involved slum demolitions (Dupont 2011).

In a study of the 2010 Vancouver Winter Olympics, Boyle and Haggerty (2011) observed that the city's Project Civil City initiative, promoted urban development in concert with intensified levels of policing and securitisation. However, they suggest that the promises by event organisers that development would bring benefits to the residents of the city were largely unrealised. Similarly, Kennelly and Watt (2011: 776) noted that measures to reduce youth crime in East London were a major policy objective before the London Olympics, recognising that 'even two years before the opening ceremonies are scheduled to begin, young people living in transitional housing in East London were encountering the revised spatial practices that also accompanied the Vancouver Olympics, carried out through intensified policing and security regimes'. There was intensification of police 'stop and search' powers in relation to young people and related 'clean up the streets' operations in preparation for the world's intensive glare. Kennelly and Watt suggest that the measures acted to stereotype youth as public order risks and that the building of Olympic infrastructure,

when coupled with increased policing measures, had a direct impact on some of the youths' everyday lives.

The UN Habitat (2007) reported that one of the main causes of large-scale forced evictions are international mega events, including global conferences and international sports events, such as the Olympic Games. Such evictions are often undertaken with bulldozers, supported by heavy police presence, and the targets are nearly always the residents of poor informal settlements or slums. The UN Habitat reported that approximately: 720,000 people were forcibly evicted in Seoul and Inchon (South Korea), prior to the 1988 Olympic Games; 30,000 forcibly evicted in Atlanta prior to the 1996 Olympic Games; hundreds were forced from their homes in preparation for the 2004 Athens Olympic Games; and 1.7 million people were reportedly evicted in Beijing (China) in the run-up to the 2008 Olympic Games (2007: 129).

Technologies for security surveillance

The provision of a safe and secure environment is of high priority for sport event owners, event venues, host cities and countries. There are pressures on these stakeholders to portray the event as having the latest and most sophisticated security and surveillance measures available. This has triggered significant growth of sport event security budgets and a corresponding expansion of security expertise and technologies. Within his analysis of mega events, Klauser (2010) has argued that host cities have responded to the demands and expectations of event owners and the public by constructing enclosed and tightly controlled enclaves that are equipped with advanced surveillance technologies and large numbers of security personnel. Further, it has been suggested that mega-events may provide platforms for

security companies to introduce and pilot new security technologies that potentially present wider benefit in society (Giulianotti and Klauser 2011).

The examples of technology related interventions are vast. Prior to 9/11, many technology advances and initiatives were spurred by attempts to quell British soccer hooligan violence, whereby CCTV systems were installed in all major football stadiums in the UK by the mid-1990s. This had significant benefit not only for game attendees but globally as the associated security surveillance was transferred to urban centres (Giulianotti and Armstrong 1998) and other sport facilities and events.

The Athens 2004 Olympic Games required significant urban development and installation of surveillance systems which created a sizeable financial burden for Greece. According to Minas Samatas, an expert of the Athens Olympic security operation, the surveillance system cost $300 million, and years after the Olympics, it remained unworkable (cited in Molnar 2011). Ironically, Science Applications International Corp (SAIC), the contractor hired to deliver a security system used during these Olympic Games, was, in 2013, awarded more than $52 million in damages and fees by an international arbitrator, who ordered Greece to pay for what the company alleged to be breach of contract. SAIC was contracted in 2003 to deliver a command, control, communications, coordination and integration system to prevent a terrorist attack during the Olympics and subsequently to serve as a security system for the Greek law enforcement community. According to SAIC, Greece used the system for two years after the Olympics, but failed to formerly declare ownership of the system or pay SAIC. Interestingly, the lack of any major security breach was more to do with the behind the scenes diplomacy between the Greek government and Muslim, Arab, Palestinian and Israeli

representatives, than the cost of the electronic surveillance system demanded by the US security and compliance lobby (Rojek 2013). However, the legacy was such that the Chinese organisers of the Beijing 2008 Olympic Games invited experts from over 70 other countries to work with them to design and implement the massive surveillance system termed the 'Golden Shield' (Samatas 2011: 3354). This involved 24/7 monitoring of citizens by CCTV cameras, Olympic radio frequency identification chips (RFID) tickets and second generation national ID cards; phone call monitoring by digital voice recognition technologies; and the 'Great Firewall' system of online censorship and filtering. In 2010, for the Commonwealth Games, 2000 CCTV cameras were installed throughout the host city of Delhi (Giulianotti 2013).

In discussing the 2006 FIFA World Cup in Germany, Eick (2011b) noted that a wide array of (FIFA-imposed) security and surveillance technologies were deployed, including airborne warning and control system planes, security robots, video surveillance cameras and RFID chips. Over 250,000 personal data files of FIFA employees and another 10 million of those persons applying for tickets were recorded. While most CCTV systems at public viewing areas were dismantled after the World Cup due to legal constraints and costs, some of the CCTV continued to operate post event. As Eisenhauer (2013) observed, the World Cup facilitated an expansion and centralisation of CCTV systems in not only the hosting sports stadia, but also in railway stations and through urban public transport networks.

For the London Olympics, anti-terrorism and crowd control measures involved the use of 'unmanned drones, surface-to-air missile systems, and a thousand armed US diplomatic and FBI agents policing an Olympic zone divided from the rest of the city by an 11-mile, £80

million 5000-volt electric fence' (Rojeck 2013: vii). Electronic surveillance included scanners, biometric ID cards, number plate and facial recognition CCTV systems, disease tracking surveillance and checkpoints.

The transfer of security personnel, knowledge and technological hardware between the host cities of sport events occurs through a range of activities, from ad hoc to systemised processes. Specific policy handbooks and guidelines (such as the 2004 EU handbook on securing against terrorist acts at major sports events), standardised procedures from the bidding process to the staging of the event and progress monitoring by the organising bodies vary between each event. In addition, a key role is played simply by the global circulation of public and private stakeholders in security matters, travelling from place to place and from event to event (Eisenhauer 2013).

Security technology is, of course, not just the reserve of global mega-events but is now a mainstay of most professional sport leagues. For example, the US National Football League's (NFL) facility and event security has been at the forefront of advances. Over 10 years ago (2001), the NFL introduced CCTV facial recognition (the FaceTrac system) for the Super Bowl. In collaboration with law enforcement databases, the FaceTrac system locates faces, allows for searches, comparisons and rapid identification. In 2012, Yankee Stadium was the first sports facility to earn recognition under the Federal SAFETY (Support Anti-Terrorism by Fostering Effective Technologies) Act. The Stadium successfully passed security tests conducted by the Department of Homeland Security, granting the Stadium immunity against lawsuits resulting from terrorist attacks (Goss, Jubenville and MacBeth 2003).

Security stakeholder partnerships & privatisation

Sport event security involves the establishment of strategic partnerships between various levels of security providers, event organisers, governments, local police, national forces and international organisations such as INTERPOL. In recent years, there has been a significant shift towards the privatisation of security and the collaboration of multinational corporations for event security. According to Control PMSC (private military and security companies), the private security industry started in the 1970s in Europe and the USA and has experienced an average growth rate of 10 per cent annually. Many security functions previously regarded as the domain of the state have been privatised and outsourced, and it has been argued that these shifts in governance and the resulting proliferation of market opportunities are closely connected to the growth of the private security industry (Eick 2006). This growth has triggered an international civil society campaign seeking to regulate the private security sector run by Control PMSC. The employment of private security contractors can present challenges, as evidenced in the London Olympics case in point below.

A case in point: London 2012 Olympic Games and G4S – the failure of a private security contractor

The London Olympics' security planning and provision created partnerships between numerous levels of security organisations, including private security agencies, police, the army, the UK Border Agency and intelligence services. London is now referred to as the most securitized Games to date and has been labelled as "lockdown London" (Milne 2012).

LOCOG had contracted G4S, a private security company to provide security at the London Olympics. Prior to the Games, the G4S Chief Executive had anticipated that the £284m contract would return a £10m profit to the company. However, two weeks prior to the Olympic opening ceremony, G4S admitted it was unable to provide the promised 10,400 security personnel. To rectify the situation, the government deployed army and police personnel to ensure security during the Games was not comprised.

G4S lost £70m on the contract and £7m in associated sponsorship costs; was given a £45m restructuring charge and paid £11m to charities, including the armed forces sports organisations. The contract failure and resultant bad publicity has had significant ramifications for G4S's reputation, with the company now in a worse competitive position than it was prior to the event.

Source: MacDonald and Hunter (2013).

For further comment on political dimension of public services having to make up for private companies shortfalls – see Grix 2013.

In the case of the London Olympics, perceptions of the risk to public order and safety were no doubt influenced by the terrorist bombings in London on 7 July 2005. These attacks occurred within 24 hours of the announcement of the successful London Olympic bid. Coaffee, Fussey and Moore (2011) suggested that the timing of the bombings provided a basis for police authorities and risk consultants to increase securitisation. Rojek (2013) argues that in the same way they did in Athens (2004) and Beijing (2008), international security and surveillance corporations lobbied that risk management provision was inadequate, subsequently increasing pressure on the IOC and allied government bodies to escalate security and surveillance budgets.

Global security firms and contractors have an increasing influence on security approaches, technologies, personnel and policies in selling their services, expertise and equipment and providing an ever increasing degree of ‘protection’ from risks. Security companies strategically use larger international sport events to showcase their products and services for broader market exposure. Boyle noted that this is particularly evident within the developing world and described this as the ‘mega-event security development nexus’ (2011: 169), which links governments, sporting bodies and the security industry.

Recent Olympic Games have epitomised the complexity of relationships between multiple security stakeholders, as evidenced in the case below of the Vancouver Winter Olympic Games.

A case in point: Vancouver 2010 Winter Olympic Games

The Vancouver Winter Olympic Games was Canada's largest ever security operation, and involved multiple stakeholders (Government of Canada 2010). There were 15,000 security personnel—4,000 members of the RCMP; 1,700 other police officers; 4,500 Canadian Forces members; and 4,800 private security personnel, 119 different police forces; security background checks on 205,000 applications for Olympic and Paralympic accreditation; and 700 police representatives from 39 countries took part in the Vancouver 2010 Integrated Security Unit International Police Visitation Program.

In 2003, the Canadian Government assigned security planning for the Games to the Royal Canadian Mounted Police (RCMP). The RCMP created the Integrated Security Unit (V2010 ISU), specifically to manage the Games' security and establish a network of security-based inter-organisational relationships. The V2010 ISU was responsible for planning and conducting security operations, uniting law enforcement and the Canadian Forces. The V2010 ISU was comprised of representatives from the RCMP and 117 other law enforcement agencies, including the Vancouver Police Department, West Vancouver Police Department, and Canadian Forces. Specialist police units were deployed for tactical and special weapons teams.

Integrated National Security Enforcement Teams (INSETs) were created. This comprised representatives from the RCMP, federal agencies including the Canada Border Services Agency and the Canadian Intelligence Service, and police services. INSETs' task was providing anti-terrorism intelligence to V2010 ISU.

Other key security stakeholders for the Games were: The Canadian Armed Forces (patrolling soldiers), The North American Aerospace Defense Command (aerospace warning and

control), The Olympic Shiprider Pilot (joint operation between the RCMP's Federal Border Integrity Program and the US Coast Guard).

Honeywell Canada was employed to provide perimeter intrusion protection services, including CCTV and other technological installations. Additional private security, Contemporary Security Canada Inc., was contracted to provide private security guards.

Brand and reputation protection

As the commercial aspects of sport events have accelerated so too have brand protection initiatives for both the event and its sponsors. It has been argued that security is now a selling point in terms of world-city place branding (Coaffee and Wood 2006). Security is no longer just concerned with the safety of people; it also encompasses safeguarding event precincts to showcase the event and sponsors' brands for commercial gain. The Government of Canada signed a Federal Covenant with the IOC to protect the Olympic and Paralympic brands which led to the introduction of Bill C-47: The Olympic and Paralympic Marks Act in the House of Commons, and the Act became law on 21 June 21 2007 to protect the Olympic and Paralympic logos and emblems from unauthorised use (Government of Canada 2010). However, a balance is needed between brand protection and over-securitisation. This was illustrated during the Beijing Olympics when some Olympic sponsors complained that stringent security measures used in the host city transformed the event into the 'no fun Games' (Boyle and Haggerty 2011).

Analysts (e.g. Eick) have suggested that event owners, such as FIFA, implement rules and regulations that unduly exploit the host environment for their own profit and security.

Looking at brand and reputation from a different angle, Babiak and Wolfe (2006) were able to demonstrate how the Super Bowl XL employed socially responsible event activities as a way to include local community groups and enhance consumer loyalty.

Media

Event security itself is now a component of the mediated spectacle of sport events with public acceptance or criticisms channelled through various forms mass media – more recently through social media. Intense media attention can actually influence the development and implementation of security measures, and shape public perceptions and expectations (Toohey and Taylor 2008). Highlighting security risks, particularly in relation to terrorism threats and violence, has been a mainstay of media reporting on mega-events such as the World Cup and the Olympics, especially from the perspective of the Western media (Atkinson and Young 2012). Media reports can assist with the legitimisation of security measures.

There was extensive media scrutiny of the massive security presence around the Olympic precinct and throughout the host city during the London 2012 Olympics. In writing for the Guardian, Graham (2012) noted that the securitisation of the London Olympics involved the deployment of more troops than the war in Afghanistan. The media also criticised the Games' large security budget with respect to the then recent funding cuts to welfare, housing and legal aid.

More recently, there was extensive media reporting of the 2013 terrorist bombing at the Boston Marathon, which was telecast live internationally. This led some media commentators

to note that the Universiade, in Kazan, the capital of Tatarstan, the World Athletic Championships in Moscow, complete with a 42-kilometer marathon through the streets of Moscow, the 2014 Winter Olympic Games in Sochi, the 2014 Russian Formula One Grand Prix auto race in Sochi, the 2017 FIFA Confederations Cup, and the 2018 FIFA World Cup would focus attention on Russia as the two alleged bombers are ethnic Chechens. In the past Chechen separatists have chosen Russian targets with the maximum media impact for terrorist acts. It has been reported that after the Boston bombings, Valentin Balakhnichyov, president of the Russian Athletics Federation, told Reuters that he was tripling the level of security protection for the August marathon through Moscow and that spectators would have to go through metal detectors to approach the course. Balakhnichyov also stated that 'At the same time, we don't want to make Moscow a ghost town' (Fyodorov 2013).

Operational risk & safety management

Risk is the possibility of loss resulting from a threat, security incident, or natural disaster. Risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function. This very broad categorisation ranges from command, control and communication, to counter-terrorism intelligence and crisis and disaster management training, through to security design and implementation and is managed through event security management plans.

In their research of two sport event organising committees, Leopkey and Parent (2009) identified fifteen risk management issues in large sporting events: financial, organising, visibility, political, infrastructure, interdependence, sport, legacy, media, participation, human resources, operations, relationships, environment, and threats. The operations category

incorporates security, crowd management, safety, health and well-being; and the issue of threats encompasses acts of terrorism.

Hanstad (2012) investigated risk management issues from the perspective of a national Olympic team before and during the 2010 Winter Olympic Games in Vancouver. The risk strategy categories identified in this study were reduction, avoidance, diffusion and relationships. As opposed to risk management literature focusing on the host or organising committee's view, Hanstad found that a participating team identified risks as more positive opportunities than negative factors.

Each sport event and its stakeholders aim to work together to mitigate risk through plans, training and communication. The Australian Grand Prix Corporation which manages the annual Formula 1 Australian Grand Prix lists its safety system elements as:

• leadership and our people;
• risk assessment and management;
• hazards and incidents;
• emergency preparedness;
• running the venue – event operations;
• running the event – event product;
• contractor management;
• design, construction and maintenance;
• working with third parties;
• information and communication;
• records and documentation; and
• monitoring and assurance (WorkSafe Victoria 2006).

Case Study: Beijing 2008 Olympic Games – The largest security budget ever at the Olympics and the role of multiple international stakeholders

The Beijing Games involved the most extensive security operations and largest security budget of any Olympic Games to date. Multiple national and international stakeholders were involved in the planning, implementation and management of security for the Games. At the national ministerial level, an Olympic Security Command Centre was established. This was co-ordinated by the Ministry of Public Security and relevant national departments, including the national armed forces.

On an international level, experts from over 70 security agencies were consulted. To manage the international securitisation of the Games, an International Police Liaison Department was established within the Security Command Centre (Yu et al 2009). BOCOG worked in collaboration with INTERPOL in the planning and preparation of security. The establishment of strategic relationships between INTERPOL, BOGOC, the Chinese authorities, and law enforcement agencies in other participating countries was a high priority in the lead up to the Games. As stated by Mr. Zhou Yongkang, State Councilor and Minister of Public Security, 'The co-operation between all the stakeholders will significantly insure the security for the 2008 Beijing Olympic Games' (quoted in INTERPOL Media Release 2007). Security during the Games involved technical and operational services from an INTERPOL Major Events Support Team.

The securitisation of the Games relied heavily on relationships with international stakeholders. In 2005, the International Permanent Observatory on Security Measures During Major Events was established. This saw 24 foreign security experts, from ten countries and four international organisations, come together to share experiences. This included personnel from the US Federal Bureau of Investigation, the United Nations' Inter Regional Crime and Justice Research Institute and the European Police Office. Regular security conferences were also organised, which established relationships for future inter-organisational collaborations (http://www.interpol.int/en).

The securitisation of the Games also relied heavily on relationships with private security and technology companies. Almost 90 per cent of expenditure on security technologies went to foreign companies. GE, IBM, HP, Dell, Panasonic and Siemens and many others were involved in providing the technology needed for the vast security operations. Security expertise and technologies from a number of foreign transnational companies was employed. These companies greatly benefitted in aftermath of the Games, in terms of further security contracts for large events.

Case Study: English football security system

Soccer/football hooliganism was perceived as a social problem in the United Kingdom in the 1980s. In response the Thatcher government sought to wage 'war' on football hooligans through a variety of approaches. Giulianotti and Klauser (2012) classified these into five domains as:

• legal, through punitive sentencing and new laws, such as the Football Offences Act 1991, and the Football Disorder Act 2000;

• bureaucratic, through more specialised policing frameworks, such as within the National Criminal Intelligence Service, which included a 'National Football Intelligence Unit' and other units investigating serious organised crime;

• bio-technological, through new security technologies and architectures to discipline and control behaviour inside stadiums; the strongest illustrations occurred inside stadiums, through all-seated stands (which served to pacify and to facilitate the monitoring of spectators), and CCTV systems;

• community policy, through the complete absence of public funding for community workers to engage with young spectators – unlike much of mainland Europe; and

• discursive-ideological, through the diffuse, negative labelling of hooligans and other 'enemies'.

Venues and Facilities

Facility design and management now take into consideration safety and security measures to minimise unacceptable behaviour, such as fan violence. For example, by restricting space around the venue for loitering, removing bleacher seating and standing/grass areas to all-seated facilities and introducing systems for designated fan seating and buffer zones. A range of stakeholders are involved in setting facility standards, for example the British Association of Chief of Police Officers (ACPO) 'developed stadium design standards to set parameters for construction and design of the ground to reduce crowd management issues and the likelihood of a terrorist attack' (Hall 2010: np).

Command and control centres allowing police to monitor areas inside and outside the stadium, technological security measures such as CCTV and FaceTrac - used to identify fans, run database searches, and send images to security personnel - are now commonplace. As are the conduct of risk assessments to determine specific risks, threats and vulnerabilities of respective venues. Assessments of each individual event are typically undertaken (Taylor and Taylor, 2011) and these may take into consideration relative intelligence for the event, historical intelligence of the event (i.e. fan rivalries, different sports), capacity of the stadium, and expected attendance (Hall 2010). This provides information for the various event stakeholders to have specific security plans. For example, the UK National Counter Terrorism Security Office (NaCTSO) has provided best practice guidelines in the following areas: access control, screening/searches, traffic and parking, CCTV, and managing event staff (National Counterterrorism Security Office 2006).

Security legacy

The escalating attention given to event securitisation has seen a number of security legacies established. Giulianotti and Klauser, (2010: 54) categorise security legacies associated with SMEs into six areas:

1. *Security technologies* that are piloted or implemented for the SMEs—for example, new CCTV or other surveillance systems in major urban centres;
2. *New security practices* which are deployed during the SME and then extended into other social fields—for example, the widespread use of contracted security officials to police the SME or involvement in partnership relationships with other national police forces or security companies;

3. *Governmental policies and new legislation* which are introduced to enhance SME security resilience and remain in force afterward—for example, new laws that restrict public association or the movement of specific individuals;

4. *Externally imposed social transformations* that have at least in part a security focus and which take hold before and after the SME—for example, the clearing of specific "undesirable" or "unloved" populations from SME spaces;

5. *Generalised changes in social and transsocietal relationships* following SME securitisation—for example, different relationships between local communities and police officials following particular incidents or security strategies at the SME; and

6. *Urban redevelopment* which has connections or consequences for SME securitisation—for example, slum clearance and rebuilding programs that are intended in part to repopulate and commodify specific inner-city localities.

Case Study: Athens Olympic Games – a failed legacy?

- The security regime for the Athens Olympic Games left a significant financial burden of Greece.
- Security spend for the Games was $1.5 billion.
- The major failure of the security operations was the C4I surveillance project. The surveillance system cost $300million and years after the Olympics it remained unworkable. lobbying interventions from the security and surveillance industry. Pressure from this quarter led to the investment of a $300 million 'super panopticon' CCTV and information system for the Athens Olympics (2004) (Samatas 2007). Graham (2012) estimates that the cost of providing security for each athlete in the Athens Games was £90,000.

Case Study: Sydney Olympic Games & Intelligent Risks – ongoing legacy for a private company

- One of the long-term legacies of the Sydney Olympic security operations was the establishment of Australian business, Intelligent Risks. The CEO of Intelligent Risks, Neil Fergus, was the Director of Intelligence the Sydney Olympic and Paralympic Games. Intelligent Risks was created from the expertise that was brought together to manage the Sydney Games Security.
- Intelligent Risks has since provided security advice to a range of mega sport events. Most recently their expertise was deployed during the planning of the London Olympics.
- Security companies such as Intelligent Risks are often one of the key stakeholders in the initial design of event venues and the early planning of security operations at international events.

SUMMARY

The wide array of actors involved in sport event security presents a complex, dynamic, inter-institutional network of stakeholders with varying interests, expectations and power (Hoye and Cuskelly 2007; Mastrogiannakis and Dorville 2013). The increase of formal risk management controls, practices and requirements is clearly evidenced, as is the seemingly constant public amplification of fear of major security problems, especially terrorism. Research on security and sport events (cf Eisenhauser 2013; Jennings and Lodge 2009; Taylor and Toohey 2011) has related this intensification to the growing commercialisation, commodification, globalisation, technologisation and media attention of selected mega-events (e.g. FIFA World Cup; Olympic Games). This in turn has led to an expectation that event

organisers should have plans and mechanisms in place to prevent all security risks, no matter how remote or unlikely these are (Clavel 2103; Spaaj 2013).

Another key theme in the literature is the debate about the standardisation of security and safety planning, practices and technologies. The homogenisation of risk management tools, policies and stadium design (Jennings and Lodge 2009), has been found to alienate spectators and fans because of restrictions placed on attendees (Paramio, Babatunde and Campos 2008; Taylor and Toohey 2011), facilitate the introduction of intrusive surveillance and control measures (Eisenhauser 2013) and herald the introduction of legislation that grants police and authorities power and control over public spaces (Giulianotti and Klauser 2011) that extend beyond the boundaries and hosting of the event itself. The ever expanding commercialisation of events has created another type of security threat – as related to marketing and branding. The ability of an event host location to provide a secure environment has even in itself become a branding point (Coaffee and Wood 2006).

The mounting level of high-intensity surveillance and large scale personnel presence (Eick 2011b; Klauser 2010) is fuelled by demands of security lobby groups (Rojek 2013) and has been linked with the shift from government provided security to the growth of use of commercial firms (Eick 2006), especially in developing countries (Boyle 2011). The influence and impact of event security and safety clearly has wider social and political implications (Yu, Klauser and Chan 2009), and the body of research on this aspect of event legacy is proving to yield some telling outcomes. Boyle and Haggerty's (2011) study of the 2010 Vancouver Winter Olympics and Kennelly and Watt's (2011) analysis of the London Olympics, both pointed to unrealised positive community benefits of event hosting as related to event associated security amplifications. Too many times we hear stories of forced evictions and local residents' relocations in the name of event safety and security. Giulianotti

and Klauser's (2010) classification of security legacies into six dimensions provides a useful framework for legacy categorisation.

CONCLUSION

With the escalation of security related interventions, some of which are incredibly costly, the question is whether the level of investment in security is a true reflection of what is needed in response to an objective security risk assessment. As we have pointed out in previous research (Taylor and Toohey 2011) excessive surveillance and control can negatively impact on spectator enjoyment and satisfaction, and can be detrimental if associated with a lack of tolerance, democracy, or respect for human rights. Security needs to be aligned with branding messages for the event, otherwise the event runs the risk of undergoing reputational damage.

SMEs may have substantial security legacies for their stakeholders. The special legislation, surveillance interventions, new policing techniques and associated urban redevelopments may all remain (Giulianotti and Klauser 2012). The following areas would benefit from future research, especially as much has been written on mega-events but there is far less information about smaller sport events (e.g. local championships).

There is scope for examining how different cultures may impact the expectations and approaches to managing security and safety issues and their importance for the different stakeholder groups. Recently, there has been a rise in the number of sport mega-events being hosted in the developing Global South. For example, the 2010 Commonwealth Games in Delhi, the 2010 FIFA World Cup in South Africa, the 2014 FIFA World Cup in Brazil and the 2016 Olympic Games in Rio de Janeiro. Hosting SMEs in these countries raises security

issues in regards to violent crime, the state's monopoly on violence and urban development (Giulianotti and Klauser 2012).

Additional research topics might include:

- The transference of responsibility for security and safety throughout the hierarchy of the stakeholders involved in the event (e.g. event owner to local organising committee to the local stakeholders).
- The effect of social media on event security.
- How is event security knowledge most effectively transferred between different types of events and stakeholders?

SUGGESTED FURTHER READING

Bennett and K.D. Haggerty (eds.) (2011). *Security games: Surveillance and control at mega-events*, Routledge, London, 169-184.

Cornelissen, S. (2011) 'Mega event securitisation in a third world setting: Global processes and ramifications during the 2010 FIFA World Cup', *Urban Studies*, 48: 3221-40.

Special Issue: Security and Sport Mega-Events: A complex relation, (2013) *Sport in Society* 16(2).

REFERENCES

Atkinson, M. & Young, K. (2012) Shadowed by the corpse of war: Sport spectacles and the spirit of terrorism‘, *International Review for the Sociology of Sport*, 7(3): 286-306.

Babiak, K., & Wolfe, R. (2006) ‘More than just a game? Corporate social responsibility and Super Bowl XL’, *Sport Marketing Quarterly*, 15: 214-22.

Boyle, P. and Haggerty, K. (2009) ‘Spectacular security: mega-events and the security complex’, *International Political Sociology*, 3: 257–274.

Boyle, P.J. & Haggerty, K.D. (2011) ‘Civil cities and urban governance: Regulating disorder for the Vancouver Winter Olympics’, *Urban Studies*, 48(15): 3185-3201.

Clavel, A. (2013) ‘Armed forces and sports mega events: an accepted involvement in a globalized world’, *Sport in Society* 16(2) pp 205-222.

Coaffee, J. Fussey, P. & Moore, C. (2011) ‘Laminated security for London 2012: Enhancing security infrastructures to defend mega sporting events’, *Urban Studies*, 48(15): 3311-27.

Coaffee, J. & Wood, D.M. (2006) ‘Security is coming home: Rethinking scale and constructing resilience in the global urban response to terrorist risk’, *International Relations*, 20(4): 503-17.

Dupont ,V. 2011 The dream of Delhi as a global city. International Journal of Urban and Regional Research. 35 (3), 533–554.

Durodie. W. (2007) ‘Miscommunicating risk: some key lessons for risk management’, A context statement presented to Middlesex University as part of the requirements for the award of a PhD by Public Works. Online. Available at https://eprints.mdx.ac.uk/6468/1/Durodie-Miscommunicating_risk.phd.pdf (accessed 1 August 2013).

Eick, V. (2006) ‘ Preventive urban discipline: Rent-a-cops and the neoliberal glocalization in Germany’, *Social Justice*. 33(3): 66-84.

Eick, V. (2011a) ‘”Secure our profits!” The FIFA in Germany 2006’, in C. Bennett and K. Haggerty (eds.), *Security games. Surveillance and control at mega-events*, New York: Routledge. 87-102.

Eick. V. (2011b) ‘Lack of Legacy? Shadows of Surveillance after the 2006 FIFA World Cup in Germany’, *Urban Studies*, 48: 3329-45.

Eick, V., & Töpfer, E. 2008, April 25. The human and hardware of policing neoliberal sportevents: Rent-a-Cops, volunteers and CCTV at the FIFA Championship in Germany 2006 and beyond. Paper presented at the conference Security and Surveillance at Mega Sport Events, Durham University, Durham, UK.

Eisenhauser, S.(2013) Managing event places and viewer spaces: Security, surveillance and stakeholder interests at the 2010 FIFA World Cup in South Africa. Unpublished PhD thesis, University of Technology, Sydney.

Fyodorov, G. (2013) ‘Entire Moscow marathon route will have metal detectors’. April 25, Reuters.) Online. Available at: http://articles.chicagotribune.com/2013-04-25/sports/chi-metal-detectors-will-be-installed-along-entire-moscow-marathon-route-20130425_1_metal-detectors-boston-marathon-luzhniki (accessed 1 August 2013).

Girginov, V. & Gold, J. (2013) *London 2012 Olympic and Paralympic Games Knowledge Transfer: A Report Prepared for Podium*. No publisher details.

Giulianotti, R. (2013) Six security legacies of major sporting events. *International Centre for Sport Security Journal.* 1(1): 94-101.

Giulianotti, R. & Armstrong, G. (1998) 'From another angle: Police, surveillance and football supporters', in C. Norris, G. Armstrong and J. Moran (eds.) *Surveillance, CCTV & social control*, Aldershot: Gower/Ashgate. 113-35.

Giulianotti, R. & Klauser, F.R. (2010) 'Security governance and sport mega-events: Towards an interdisciplinary research agenda', *Journal of Sport & Social Issues*, 34: 49-61.

Giulianotti, R. & Klauser, F.R. (2011), 'Introduction: Security and surveillance at sport mega events', *Urban Studies*, 48: 157-68.

Giulianotti, R., & Klauser, F. (2012). Sport mega-events and 'terrorism': A critical analysis. *International Review for the Sociology of Sport*, 47: 307-323.

Goss, B.D., Jubenville, C.B. & MacBeth, J.L. (2003) Primary Principles of Post-9/11 Stadium Security in the United States: Transatlantic Implications from British Practices. Online. Available HTTP: www.iaam.org/CVMS/Post%20911%20Stadium%20Security.doc. (accessed 1 August 2013).

Government of Canada (2010) 'Canada's Games: The Government of Canada and the 2010 Vancouver Olympic and Paralympic Winter Games'. Her Majesty the Queen in Right of Canada. Online. Available HTTP: http://www.fin.gov.bc.ca/reports/Canadareport.pdf (accessed 1 August 2013).

Graham, S. (2012) 'Olympics 2012 security: Welcome to lockdown London'. *The Guardian*. Online. Available HTTP: http://www.guardian.co.uk/sport/2012/mar/12/london-olympics-security-lockdown-london (accessed 12 March 2012).

Grady, J., McKelvey, S. & Bernthal, M.J. (2010) 'From Beijing 2008 to London 2012: Examining event-specific Olympic legislation vis-à-vis the rights and interests of stakeholders', *Journal of Sponsorship*, 3: 144-56.

Grix, J. (2013) 'Sport Politics and the Olympics', *Political Studies Review*, 11: 15-25.

Haferburg, C. (2011) 'South Africa under FIFA's reign: The World Cup's contribution to urban development', *Development Southern Africa*, 28: 333-48.

Hall, C.M. (2006) 'Urban entrepreneurship, corporate interests and sports mega-events: The thin policies of competitiveness within the hard outcomes of neoliberalism', *Sociological Review*, 54(2): 59-70.

Hall, S. (2010) 'An Examination of British Sport Security Strategies, Legislation, and Risk Management Practices', *Sport Journal*, 13(2) (unpaginated).

Hanstad, D. (2012) Risk management in major sporting events: A participating national Olympic team's perspective. *Event Management*, 16 (3): 189-201.

Hoye, R. & Cuskelly, G. (2007) *Sport Governance*, Oxford: Elsevier.

International Olympic Committee (2012a) *Report of the IOC 2020 Evaluation Commission Games of the XXXII Olympiad*, Lausanne: IOC.

International Olympic Committee (2012b) 2012 *2020 Working Group Report / Games of the XXXII Olympiad*, Lausanne: IOC. Online. Available at HTTP: http://www.olympic.org/Documents/Host_city_elections/Final-report-2020-Working-Group-English.pdf (accessed 1 August 2013).

Jennings, W. & Lodge, M. (2009) 'Governing mega-events: tools of security risk management for the London 2012 Olympic Games and the FIFA 2006World Cup in

Germany' Paper presented at the 59th Political Studies Association, Manchester, 9 April. Online. Available HTTP: http://www.academia.edu/209696/Governing_Mega-Events_Tools_of_Security_Risk_Management_for_the_London_2012_Olympic_Games_and_FIFA_2006_World_Cup_in_Germany (accessed 1 August 2013).

Johnson, C. W. (2006) 'A Brief Overview of Technical and Organisational Security at Olympic Events', Working paper Department of Computing Science, University of Glasgow, Glasgow, Scotland, UK : 1-24. Online. Available HTTP:http://www.dcs.gla.ac.uk/~johnson/papers/CW_Johnson_Olympics.pdf (accessed 26 May 2010).

Kennelly, J. & Watt, P. (2011) 'Sanitizing Public Space in Olympic Host Cities: The Spatial Experiences of Marginalized Youth in 2010 Vancouver and 2012 London', *Sociology,* 45: 765-781.

Klauser, F.R. (2010). Splintering spheres of security: Peter Sloterdijk and the fortress city,' *Environment and Planning D: Society and Space.* 28: 326-340.

Leopkey, B. & Parent, M.M. (2009) 'Risk management issues in large-scale sporting events: A stakeholder perspective', *European Sport Management Quarterly*, 9: 187-208.

MacDonald, M. & Hunter, D. (2013) 'The discourse of Olympic security 2012: London 2012'. *Discourse and Society*, 24: 66-88.

Mastrogiannakis, D. and Dorville, C. (2013) 'Security and sport mega-events: a complex relation', *Sport in Society,* 16: 133- 139.

Milne, S. (2012) 'This is a Corporate Lockdown, Why Not an Olympics for All?', The Guardian. 11 July. Online. Available HTTP:

http://www.theguardian.com/commentisfree/2012/jul/10/london-olympics-lockdown-2012-games (accessed 1 August 2013).

Misener, L., and Mason, D. (2009) 'Fostering Community Development Through Sporting Events Strategies: An Examination of Urban Regime Perceptions', *Journal of Sport Management*, 23: 770-94.

Molnar, A. (2011) 'Warning to London 2012 Olympic hosts as Greece struggles with economy and security: an interview with political sociologist Minas Samatas'. 15 August. Online. Available HTTP: http://www.security-games.com/news/warning-to-london-2012-olympic-hosts-as-greece-struggles-with-economy-and-security (accessed 1 August 2013).

National Counterterrorism Security Office. (2006) 'Counter Terrorism Protective Security Advice for Stadia and Arenas'. Association of Chief Police Officers in Scotland. Online. Available HTTP: http://nactso-dev.co.uk/system/cms/files/121/files/original/Stadia___Arenas_2011.pdf (accessed 1 August 2013).

Paramio, J., Babatunde, B., & Campos, C. (2008) 'From modern to postmodern: the development of football stadia in Europe', *Sport in Society*, 11: 517- 534.

Parent, M. (2008) 'Evolution and issue patterns for major-sport-event organizing committees and their stakeholders', *Journal of Sport Management*, 22: 135-164.

Rojek, C. (2013) *Event Power: How Global Events Manage and Manipulate*. London: Sage.

Samatas, M. (2007). 'Security and surveillance in the Athens 2004 Olympics: Some lessons from a trouble story.' *International Criminal Justice Review* 17 (3): 220-238.

Samatas, M. (2011) 'Surveillances in Athens 2004 and Beijing 2008: A Comparison of the Olympic Surveillance Modalities and Legacies in Two Different Olympic Host Regimes', *Urban Studies*, 48: 3347-66.

Spaaij, R. (2013) 'Risk, security and technology: governing football supporters in the twenty-first century', *Sport in Society* 16: 167- 183.

Sweaney, K. (2005) 'Ready for Anything', *Australasian Leisure Management* 53: 22–30.

Taylor, T. L. & Toohey, K. (2011) 'Ensuring Safety at Australian Sport Event Precincts: Creating Securitised, Sanitised and Stifling Spaces?', *Urban Studies*, 48: 3259-75.

Toohey, K. & Taylor, T. L. (2008) 'Mega Events, Fear, and Risk: Terrorism at the Olympic Games'. *Journal of Sport Management*, 22: 451-469.

Toohey, K & Taylor, T. L. (2012) 'Surveillance and securitization: A forgotten Sydney Olympic legacy'. *International Review for the Sociology of Sport*, 47: 324-337.

Un-Habitat (2007) *Enhancing urban safety and security: Global report on human settlements*. Nairobi, Kenya United Nations Human Settlements Programme. Online. Available HTTP: http://www.unhabitat.org/downloads/docs/GRHS.2007.0.pdf (accessed 1 August 2013).

WorkSafe Victoria (2006) *Advice for managing major events safely*. Melbourne: State Government of Victoria. Online. Available HTTP: http://www.worksafe.vic.gov.au/__data/assets/pdf_file/0010/12502/major_events_organisers_advice.pdf (accessed 1 August 2013).

Yu, Y., Klauser, F. & Chan, G. (2009) 'Governing security at the 2008 Beijing Olympics', *International Journal of the History of Sport*, 26: 390-405.

Table 1

Stakeholder Interventions

Stakeholder					
Event Owner	**Local Organising Committee**	**Event Sponsor /Sport Facility**	**State or National Government**	**Security Firms/ Police and emergency services**	**Media**
Initial event hosting application assessment of security operation	Assessment of relevant risk registers, risk management plans, event safety plans	Crowd management strategies e.g. restrictions on alcohol sales	Legislation	Surveillance technology	Social media communication
Restrictions on commercial access	Restrictions on public access	Surveillance technology and facility design	Installation and use of surveillance technology	Law enforcement	Reporting & information dissemination
Brand protection	Requiring permits and adherence to local ordinances	Brand protection	Brand protection	Increase the visibility of security	
Contractual agreements	Contractual agreements	Contractual agreements	Urban planning/ development	Remove and/or isolate aggressive spectators	
	Training event personnel – paid and volunteers	Operational Risk & Safety management / Hazard Plans	Refuse entry to known and potential troublemakers		
	Internal risk planning committee	Internal risk planning committee	Risk planning committee		