Governing mega-events: tools of security risk management for the London 2012 Olympic Games and FIFA 2006 World Cup in Germany

Will Jennings, School of Social Sciences, University of Manchester (will.jennings@manchester.ac.uk)

Martin Lodge, Department of Government & ESRC Centre for Analysis of Risk and Regulation, London School of Economics and Political Science (m.lodge@lse.ac.uk)

Paper for the 59th Political Studies Association Conference, Manchester, 8 April 2009

Acknowledgements: Will Jennings thanks the UK Economic and Social Research Council for support through the ESRC Research Fellowship (ESRC Reference RES-063-27-0205), 'Going for Gold: The Olympics, Risk and Risk Management'.

Copyright PSA 2009

Abstract

Sporting mega-events such as the Olympic Games and football World Cups represent a special venue for the practice of risk management. The risk profile of sporting mega-events appears to conflict with the supposed risk-averse and blame-avoiding tendencies of contemporary policy-makers and bureaucrats, who instead pursue 'high risk, high gain' strategies in bidding for and hosting Olympic Games, football World Cups, and the like. This paper proposes a framework for analysis of security risk management, based on the 'tools of government' approach (Hood 1983, Hood and Margetts 2007). It considers those tools in the context of two sporting mega-events: security risk management for the London 2012 Olympic Games and for the FIFA 2006 World Cup in Germany.

Copyright PSA 2009

Introduction

Theories and the practice of risk and crisis management have received considerable attention from political science and wider social science literatures, in recent times.[1] Whether focused on analysis of steps to mediate potential crises or approaches to handling post-crisis situations, the political dimension of risk and crisis management has become prominent, with particular interest in prominent cases such as Hurricanes Katrina or September 11th, 2001.[2] The management of risk at major international sporting events, such as the Olympic Games, has likewise been subject to recent analysis.[3]

Most of these studies draw general inferences from tracing processes of decision-making during particular crises situations, comparing cases in different contexts and over time. In this paper, we develop a different perspective. The analysis focuses upon categorisation of tools of security risk management and compares their application across two mega-events: the London 2012 Olympics and the FIFA 2006 Football World Cup in Germany. Such a comparison also allows for discussion of a wider question: how can we understand the selection and use of risk management tool-sets? According to the advice of risk management manuals, there should be a differentiated response that reflects the functional demands of specific events and risk profiles. According to the organisational literature, processes of institutional isomorphism[4] are expected in which dominant forms of risk management travel and diffuse.

We explore the analysis of this question through the 'tools of government' perspective, developed by Christopher Hood,[5] using this analytical approach to compare the management of security risks at two mega-events: the bid and preparations of the London 2012 Olympics and organisation of the FIFA 2006 Football World Cup in Germany. Both of these sporting events exhibit attributes of a mega-event (a concept that is considered further below) because of their exceptional scale and scope and long-term resource commitment, in particular as regards construction of infrastructure (e.g. public transport) and facilities (e.g. stadia, accommodation) but also in terms of operations. The complex interdependence of infrastructure and operations at sporting mega-events makes them high risk, when compared with regular athletics meetings or football league competitions. Mega-events therefore represent a site for all kinds of organisational and technological failures, combined with elevation of the threat level from terrorist incidents (and indeed diplomatic incidents) due to the global profile of events such as the Olympics and the World Cup.

---

[1] Stephen Breyer. (1993). Breaking The Vicious Circle: Toward Effective Risk Regulation. Cambridge, Massachusetts: Harvard University Press; Christopher Hood, Robert Baldwin and Henry Rothstein. (2001). The Government of Risk. Oxford: Oxford University Press; Power, M. (2004). The Risk Management of Everything. London: Demos; Power, M. (2007). Organized Uncertainty: Organizing a World of Risk Management. Oxford: Oxford University Press; Paul 't Hart and Mark Bovens. (1996). Understanding Policy Fiascoes. New Brunswick: Transaction Publishers; U. Rosenthal, M.T. Charles and Paul 't Hart (eds.) (1989). Coping with Crises: The Management of Disasters, Riots and Terrorism. Springfield, Illinois: Charles C. Thomas.

[2] Boin, A, McConnell, A, and t'Hart, P (2008) Governing After Crisis, Cambridge, Cambridge University Press. Boin, A, t'Hart, P, Stern, E and Sundelius, B (2005) The politics of crisis management, Cambridge, Cambridge University Press.

[3] E.g. Will Jennings. (2008). 'London 2012: Olympic Risk, Risk Management, and Olymponomics', John Liner Review 22 (2): 39-45; Will Jennings and Martin Lodge. (n.d.). 'London 2012: Critical infrastructures and the politics of resilience', working paper; Will Jennings and Martin Lodge (n.d.). 'The Olympic Games: coping with risks and crises at a mega-event', working paper to be published in Uriel Rosenthal, Brian Jacobs, Louise K. Comfort, Ira Helsloot (eds.) Mega-Crises (Charles C Thomas, Springfield Ill.).

[4] DiMaggio, P and Powell, W (1991) 'The Iron Cage Revisited' in P. DiMaggio and W. Powell (eds) The new institutionalism in organisational analysis, Chicago, Chicago University Press.

[5] Hood, C (1983) Tools of Government, Basingstoke, Macmillan. Hood, C and Margetts, H (2007) Tools of Government in a Digital Age, Basingstoke, Palgrave Macmillan.

Copyright PSA 2009

At the same time, the hyper-political and symbolic attributes of such mega-events are symptomatic of grand projects associated with high modernist regimes,[6] as well as the synoptic control tendencies of contemporary styles of organisation and governing. Governance of sport at the international is subject to all sorts of geo-politics, while domestic politics can permeate the staging of mega-events as national and sub-national governments vie for influence and as different public agencies compete for resources. There is sufficient similarity in the risk profiles of the two mega-events to enable comparisons, but sufficient difference to diagnose the relative homogeneity or heterogeneity of risk management responses.

The remainder of this paper proceeds in three stages of analysis. First, it introduces the tools of government approach and considers the theoretical basis of two central hypotheses: differentiation and isomorphism. Second, it outlines the distinct risk profile of the two mega-events, the London 2012 Olympics and FIFA 2006 World Cup in Germany, and theoretical expectations are derived with regard to tools of risk management. Third, it compares different approaches to security risk management at the two mega-events through the tool perspective, before concluding with general assessment of trade-offs and side effects of different approaches to risk management at mega-events.

Tools of security risk management

As an alternative to the evaluation of decision-making processes, the following section considers a conceptual typology for categorisation and analysis of generic instruments utilised in dealing with particular security risks. It first explores the fourfold theoretical distinction of 'tools of government' introduced over twenty-five years ago by Christopher Hood. Second, it considers two contrasting explanations regarding tool choice: differentiation and isomorphism.

Although there have been numerous attempts at the conceptualisation of policy tools or instruments[7] – most of them born from a desire to establish generic categories for comparison of similarities or differences in policy interventions in light of similar problems – the tools of government perspective developed by Christopher Hood offers significant advantages in its parsimony and transparency. Hood's theoretical (cybernetically-informed) framework offers a critical lens for the categorisation and analysis of different tools through which government interfaces with society.[8] This approach therefore enables a parsimonious perspective on the resources available to policy-makers for gathering information and modifying the behaviour of its citizens. The government toolbox – of nodality, authority, treasure, and organisation ('NATO') – constructed by Hood and brought into the digital age by Hood and Margetts,[9] is outlined in Table 1.

[6] James C. Scott. (1998) Seeing Like A State, New Haven, Yale University Press.
[7] Stephen H. Linder and B. Guy Peters. (1989). 'Instruments of Government: perceptions and contexts', Journal of Public Policy 9(1): pp.35-58; Lester Salomon. (2002). The Tools of Government: A Guide to the New Governance. Oxford: Oxford University Press; Christopher Hood. (2007). 'Intellectual Obsolescence and Intellectual Makeovers: Reflections on the Tools of Government after Two Decades', Governance 20(1): pp.127-144.
[8] Christopher Hood. (1983). The Tools of Government. London: Macmillan.
[9] Christopher Hood and Helen Margetts. (2007). The Tools of Government in the Digital Age. London: Palgrave Macmillan.

Copyright PSA 2009

Table 1: The tools of government (from Hood 1983, Hood and Margetts 2007)

Treasure Reliance on exchange of goods and money	**Nodality** Reliance on being in the middle of an information network
Organisation Reliance on ability to act directly	**Authority** Reliance on possession of legal authority

Nodality denotes the extent to which government is a central point or node of contact in information networks. This describes its capacity to receive and send information as well as to use information (propaganda) to modify the behaviours of actors. Translated into the world of security risk management, nodality refers to those instruments that facilitate information exchange between police and security services concerning the whereabouts and intentions of particular individuals or groups. It also refers to collection and analysis of intelligence about threats, spectators and traffic flows and understanding of network peaks and bottlenecks in order to redirect traffic and to mobilise 'organisation' to avoid problems. This can be equated with both counter-terrorism and 'intelligent policing'. At the same time, nodality relies on technical devices such as centralised and interconnected databases to check ticketing and visiting data, especially at the various points of entry into a country (e.g. border controls). Nodality also includes the use of public information for visitors and citizens about security issues, encouraging grassroots alertness and reporting of suspect activity or incidents.

Authority refers to the legal power of government and other sources of legitimacy. This refers to those tools that enable government, at all levels, the right to license, to demand or to prohibit certain activities. This includes censorship and procedural devices to limit demonstrations, as well as legal authority to deal with ticket touts, day-to-day criminal activities, prostitution, licensing of drinking establishments (in terms of hours and menu choices), and measures to impede the movement of dangerous (i.e. high risk) groups or individuals such as hooligans. Overall, authority extends to the authorization of planning permission and imposition of health and safety standards; for example with reference to the design and construction of sporting facilities or critical infrastructures (i.e. transport, energy, communications and water networks).

Treasure denotes the access of government to assets and financial resources. This is often observed as financial subsidies and tax receipts that modify individual behaviour. In the context of security risk management, use of 'fungible chattels' concerns the application of financial strength for purposes of direct expenditure on security or indirect provision of insurance and assurance services (with the government acting as lender of last resort). This also refers to public spending on construction and operation of buildings, such as stadiums, into which security capacity and responses can be hardwired through design or architecture. Treasure is also required for payment of mercenaries: e.g. private security firms contracted to provide support for public security and defence services and funding of third-sector emergency services (charities) that are not direct part of the government apparatus, but exist somewhere in the twilight zone between public and private sectors.

Last, organisation refers to the capacity of government for undertaking direct action, for example in its mobilization of bureaucrats or the armed forces. This refers to the physical ability of government to intervene in the affairs of its citizens or other states or otherwise to act as a deterrent (rather than reliance upon brute strength in policing). As such, it concerns the direct presence of security services but extends to design and configuration of event architecture in a broader sense and operation of technologies of social control (that sometimes intersect with information-gathering functions). This includes devices that reduce bottlenecks,

Copyright PSA 2009

such as in the case of transportation, or create them, such as in the management of visitor flows and exercise of entrance controls ('turnstiles'). Likewise it refers to the setting of boundaries or construction of perimeters to separate groups or demarcate a particular area as subject to special security status.

Among the many theories as to why particular instruments or tools are chosen in the type of contexts such as that for mega-sporting events, two critical theories are those of functional differentiation and institutional isomorphism. According to the former,[10] tools are chosen depending on the functional requirements and the risk profile of the particular event. Based on the assumption that governments will seek to economise on their resource-use, i.e. governments prefer to use less coercive and fewer depletable resources in the light of given challenges, we can assume that the responses to the Olympics and the football World Cup will be different in the light of different functional demands, as explored below. Similar observable implications would also follow from a perspective that would assume high degrees of rationality: in other words, decision-makers would frame their tools in the light of carefully (and systematically gathered) information, an assessment of their target populations as well as a consideration of the type of standards in terms of safety they want to achieve. In other words, this perspective assumes that decision-makers will not economise on rationality, but rather develop tools to provide for as comprehensive a perspective on the given security risks associated with a mega-event as possible. Given the differences in risk profile, we should therefore, similarly, expect differences in the utilisation of tools for security risk management. This has some overlap with the rationale of modern regulatory governance and the rolling back of state intervention, and – until the emergence of the global financial crisis – the popularity of 'risk-based' approaches to market regulation.

In contrast to arguments that emphasise bespoke measures, other accounts, usually drawn from the wider organisational literature, emphasise the diffusion of 'off the shelf' solutions. According to DiMaggio and Powell's argument underlying 'institutional isomorphism,'[11] homogeneity of responses within similar (mature) organisational fields is to be expected. There is much to be said for such a perspective in the context of security risk management. First of all, 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 the risk management consultocracy over the past decade or so, we can also expect risk management tools to travel across domains, thereby performing, what DiMaggio and Powell call, normative source 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 it is also not difficult to find such sources that potential apply for the security risk management of major sporting 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 Sports Events*, especially in football.

In the following analysis, we emphasise these two contrasting perspectives. Of course, comparing sporting mega-events requires acknowledgement of the context of two national political systems with contrasting political-institutional features. We will assess the impact of this factor in the conclusion. Table 2 summarises the discussion in this section, pointing to two

[10] See discussion in Hood (1983) and Hood and Margetts (2007) regarding different principles underlying too choice.
[11] DiMaggio, P and Powell, W (1991) 'The Iron Cage Revisited' in P. DiMaggio and W. Powell (eds) The new institutionalism in organisational analysis, Chicago, Chicago University Press.

Copyright PSA 2009

aspects of our analysis, first the type of observable implications in terms of what sort of tool set to expect; and second, to explore the operation of distinct mechanism.

Table 2: Overview

Mechanism	**Observable Implication**
Risk profiles require different responses in terms of economising on tool depletion	Differentiation in tool utilisation in security risk management
Risk profile imposes different functional requirements	
Apparently successful templates are emulated in conditions of high uncertainty	Similarity in tool utilisation in security risk management
Dominant professional understandings provide for templates for tools in risk security management	

Sporting Mega-Events and Risk

So what defines a mega-event and its associated risk management challenges? How different, if at all, are the challenges that are involved in managing risk at sporting mega-events such as the London 2012 Olympics or the 2006 FIFA World Cup? And why do sporting mega-events deserve specific attention as a venue for the practice of security risk management?

Although there is longstanding disagreement over what constitutes a mega-event (also known in some circles as a hallmark event),[12] it is practicable for the purpose of analysis here to accept the definition that these are "… short-term events with long-term consequences for the cities that stage them … associated with the creation of infrastructure and event facilities often carrying long-term debts and always requiring long-term use programming."[13] Mega-events are exceptional in scale and scope, consisting of an extensive and parallel programme of events, often reliant upon construction of new infrastructure and facilities (i.e. mega-projects of some sort[14]), and requiring an escalation of normal levels of public and private sector operations such as air and rail transport services, policing and fire and ambulance services. Distinct even from major public concerts and one-off sports events such as Grand Nationals or FA Cup Finals, these vast commitments to infrastructure and operations are subject to an immovable schedule of ceremonial and sporting events. Most mega-events are associated with some interruption to normal daily services, either as commuter transport trains become spectator-dominated, roads are closed, or as police and other public services are diverted to the mega-event. Such events exist, moreover, in a heightened state of attention and alert with, for example, some 4.7 billion viewers of the television coverage of the Beijing 2008 Olympics.

Mega-events might be considered as presenting something of an 'impossible job'[15] for policy-makers and organizers in the sense that they entail intractable trade-offs, blind spots and

[12] Hall, Colin M. (1989). 'The Definition and Analysis of Hallmark Tourist Events', GeoJournal 19(3): 263-268.
[13] Maurice Roche. (1994) 'Mega-Events and Urban Policy', Annals of Tourism Research 21(1): 1-19, p.1.
[14] Alan A. Altshuler and David Luberoff. (2003). Mega-projects: The changing politics of urban public investment. Washington, DC: Brookings Institution; Bent Flyvbjerg, Nils Bruzelius, and Werner Rothengatter. (2003). Megaprojects and Risk: An Anatomy of Ambition. Cambridge: Cambridge University Press; Bent Flyvbjerg, Mette K. Skamris Holm, and Søren L. Buhl. (2002). 'Underestimating Costs in Public Works Projects: Error or Lie?' Journal of the American Planning Association 68 (3): 279-295.
[15] Hargrove, EC and Glidewell, JC. (1990). Impossible Jobs in Public Management. Lawrence, KS: Kansas University Press; Arjen Boin and Paul 't Hart. (2003). 'Public Leadership in Times of Crisis: Mission Impossible?' Public Administration Review 63(5): 544-553.

Copyright PSA 2009

ambiguities; in the prioritisation of specific risks, in the selection of particular indicators to monitor and evaluate information about risks, and in use of certain policies or organizational instruments to modify behaviour (and therefore affect outcomes).[16] And even though risk management in all forms is confronted by the balancing of different priorities, mega-events represent a special test for a number of reasons. Most of all, mega-events exhibit an inherent tension between the politicized, centralizing and high risk characteristics of such events and the claimed decentralizing, risk-averse and blame-avoiding tendencies said to be widespread across contemporary governance.[17] Ironically, the attractions of hosting public spectacles and the rise of the regulatory state, understood here as attempts at imposing synoptic and regularised aspirations of design, measurement and control, lead to a type of constellation that resembles Charles Perrow's suggestion that particular industries combine tragic choices when trying to deal with normal accidents. Namely, demands for decentralised co-ordination to deal with risks need to be combined with contradictory demands for synoptic and centralised control.[18] Beyond this macro-level question of security risk management, there are further key aspects that emphasise the highly problematic nature of mega-events for developing strategies for risk management.

First, the competitive process for selecting/locating once-in-a-generation events such as the Olympics or the World Cup encourages unrealistic or over-optimistic bids. At the same time, it is also susceptible to vote-trading as part of the international diplomacy that goes hand-in-hand with such decisions. As a result, mega-events are often conceived with a view to 'win first and ask questions later'. This is manifested in the replacement of bid teams (often dominated by PR professionals, sporting ambassadors and political fixers) with infrastructure and operation teams tasked with project delivery. It is also evident in the oft-noted dissonance between the 'fiction' of bid documents[19] and hard realities of project management. For example, the public cost of the Sydney 2000, Athens 2004 and London 2012 Olympics each outreached original estimates, despite technical forecasting and budget controls. In formative bid stages, ideas concerning risk management tend to be regarded as solvable or are deferred for future consideration. The ARUP report for the London bid argued that less quantifiable Olympic risks such as those attached to security, transport and construction should inform "the decision whether or not to bid," while being offset "… against the opportunities to avoid or mitigate risk through management, anticipation, and planning".[20] The discounting and filtering out of risk information can continue throughout the course of planning and operation of a mega-event, in particular for events such as the Olympics that are in a state of permanent crisis due to challenging project deadlines, political criticism and the continuous emergence of problems.

The selection procedures for host countries and/or cities also generate sub-optimal (risky) venue/organizer choices, through politicization or distortion of decision-making and vote allocation. While there is increasing formalisation of application requirements and

---

[16] This is subject to the same general kinds of cognitive and institutional biases ('friction') of attention identified in the model of disproportionate information processing, see Bryan D. Jones and Frank R. Baumgartner. (2005). The Politics of Attention: How Government Prioritizes Problems. Chicago: University of Chicago Press.

[17] Morris P. Fiorina. (1982). 'Legislative choice of regulatory forms: Legal process or administrative process?'. Public Choice 39(4), pp.33-66; R.R. Lau. (1985). 'Two Explanations for Negativity Effects in Political Behavior'. American Journal of Political Science 29(1), pp.119-138; R. Kent Weaver. (1986). 'The Politics of Blame Avoidance'. Journal of Public Policy 6(4), pp.371-398; Christopher Hood. (2002). 'The Risk Game and the Blame Game'. Government and Opposition 37(1), pp.15-37.

[18] Charles Perrow. (1984) Normal Accidents: Living with High-Risk Technologies, New York: Basic Books; Perrow, C (1999) Normal Accidents: Living with High-Risk Technologies, Princeton: Princeton University Press, Second Edition.

[19] Dick Pound. (2004). Inside the Olympics. Toronto: John Wiley & Sons.

[20] ARUP/Insignia Richard Ellis. (2002). London Olympics 2012: Executive Summary, 21 May 2002.

Copyright PSA 2009

formats for prospective hosts, bid assessments and ongoing evaluation of progress with preparations (such as IOC Coordination Commission reports on host cities), use of secret ballots and transferable vote systems for award of the mega-event can lead to the discounting of future risks. This can result in selection of high risk bids. For example, the IOC's multiple transferable vote system for awarding the Games means the first round last-place loser is eliminated even if it would have won a majority of votes in later rounds through allocation of second, third and fourth preferences. Such institutional structures create scope for politicization, through the power of regional blocs and potential for vote-trading. The patriarchal leadership of international sporting organizations such as the IOC and FIFA over long periods of time (e.g. Juan Antonio Samaranch IOC President 1980-2001, João Havelange FIFA President 1974-1998) also cultivates personal coalitions, further detaching voting preferences from risk evaluation. This has been associated with allegations of corruption,[21] such as for the award of the Sydney 2000 and Salt Lake City 2002 Olympics.

Second, mega-events have quite an exceptional risk profile because of their iconic nature and global brand, attracting a worldwide television audience of billions, millions of spectators, and wide-ranging public and media interest. This creates the ideal platform for all sorts of grievances and rent-seeking. For example, essential workers in public services or project delivery acquire increased negotiating leverage through strike threats, while security professionals outline the range of security risks that need to be solved. At the same time, certain groups or individuals (anarchists, anti-globalisation protesters, terrorists) advertise their intentions to interrupt staging of the event, while other threats just consist of intelligence chatter. Thus, management of security risks is confronted with the choice of which risks to discount, which risks to monitor, and which risks to mitigate and protect against. Those decisions occur within a state of genuine uncertainty as to the likelihood of occurrence of a particular incident.

Third, mega-events (and events such as the Olympic Games and the Football World Cup in particular) allow little room for things to go wrong and little scope for adapting in response to external attacks or system failures. That is both in terms of managing day-to-day operational risks of ensuring the continuity of power/water supplies and transport linkages as well as attempting to avert major security disasters. Opening ceremonies and competition venues are often fixed years in advance, creating added pressure for things to be 'alright on the night', while it can be difficult to recover reputational standing and public confidence in the short-term. As is discussed later, effects of security risks on mega-events vary to some degree. For example, events at the Olympics are concentrated at the main site whereas international football tournaments tend to be spread between a number of locations, increasing the number of potential trouble spots and requirements of security coverage but dispersing risks and the probability of critical breakdowns.

While the symbolic importance of sporting mega-events generates a heightened state of attention, the large volume of spectators and participants also provide a target for common, everyday, forms of crime: such as pick-pocketing and theft, drug dealing, distribution of fake tickets and the sale of counterfeit merchandise. It is also claimed that the influx of visitors associated with some international sporting events is a contributing factor to the trafficking of prostitutes.[22]

---

[21] Vyv Simson and Andrew Jennings. (1992). The Lord of the Rings: power, money and drugs in the modern Olympics. Toronto: Stoddart; Andrew Jennings. (2006). FOUL! The Secret World of FIFA: Bribes, Vote-Rigging and Ticket Scandals. London: HarperSport.

[22] E.g. European Parliament Debates. (12 June 2006). Debate on forced prostitution during the football World Cup. O-0054/2006, http://www.europarl.europa.eu/omk/sipade3?L=EN&OBJID=120219

Copyright PSA 2009

There are, nevertheless, considerable differences between sporting mega-events in their various forms. For example, international football tournaments tend to be associated with public disorder, violence and organised hooliganism; with large crowds of national (and sometimes local) supporters that gather for specific matches during the course of concentrated periods of competition. This contrasts with the Olympics where most of the events attract a large number of spectators, but where those tend to comprise diverse/transnational audiences that do not divide their support across different teams that symbolize 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 way in which they are likely to be realised varies quite significantly.

There are also differences in organizational scale and complexity. London 2012 presents an unprecedented examination for the practice of risk management of sporting events in the UK: hosting a total of 26 sports at 31 competition venues over 17 days of competition, bringing together (an estimated) 204 participating nations, 10,500 athletes, 6,000 coaches and officials, 20,000 media, with around 500,000 visitors a day to competition venues. The Games is to be policed by around 15,000 police officers along with 7,500 private security staff (at current estimates). This task is of a different order from organization of the last major football tournament held in the UK, Euro '96: which hosted 31 games at 8 venues over 21 days of competition, with 16 participating teams, around 500 players and 100 VIPs and dignitaries, requiring 18,500 security personnel to police a total of over one million spectators. As such, football tournaments tend to be more intensive in terms of manpower, whereas the programme of Olympic events presents a complex architecture of logistical and security arrangements that is more sprawling and fluid in nature.

A further difference is location. In general, international football tournaments tend to be more resilient in response to shocks; as games are decentralised to multiple regions, towns and stadia, thereby reducing the risk that a critical breakdown or incident in one location will cause system-wide disruption. At the Olympics, a significant proportion of events are held on or near to the main site (which for recent Games has consisted of the athletics stadium, aquatics centre and the athletes' village, i.e. accommodation) at specialist venues. The technical requirements of venues are a significant determinant of the criticalness of security incidents. While there are in the region of forty football grounds in the UK with capacity for somewhere between 20,000 and 40,000 spectators, there are just two Olympic standard swimming pools. A football pitch is a football pitch after all.

As a consequence, a one-off disturbance of security – whether technological, natural, or man-made in origin – has the capacity to disturb the staging of an Olympics more extensively than a similar breach at a football tournament. Furthermore, a concentration of most blue-ribbon athletics events and the opening and closing ceremonies (which attract the largest television audiences), at a single, central venue makes the symbolic (and reputational) effects of breakdowns in security all the more powerful.

For international football tournaments, the relative decentralization of individual games means that spectators descend upon locations for a concentrated period of time, meaning that large numbers of people need to be transported between locations before and after each game. The increased volume of passenger traffic increases strain upon infrastructure and introduces additional risks for management of transport hubs and links. Often, given the more recent fashion for public viewings on giant screens in town centres and the official licensing of public overflow zones for events, such as fan miles, additional security is required to cope with the unpredictable numbers of spectators outside stadiums and in nearby urban centres and districts. This places a further strain on policing and emergency services. As witnessed in the

Copyright PSA 2009

case of Glasgow Rangers' supporters rioting and attacking local police during the UEFA Cup final in Manchester in May 2008, a key trigger was crowd agitation about the breakdown of the broadcast link to the public viewing stage in the city centre. A more benign example of the requirement for expanded security provision in such circumstances was the Dutch 'invasion' of Berne during the European Championship in June 2008, where the arrival of over 150,000 supporters meant that local restaurants ran out of food long before kick-off.

In terms of risk management, there are therefore important differences in the security uncertainties and threats that confront the organizers of sporting mega-events. In the case of the Olympic Games, these tend to concern geo-political conflicts and domestic or international terrorism, whereas the large crowds of national supporters associated with international football tournaments (mostly sympathising with opposing teams) tend to create security risks that are manifested in public disorder, and that are based upon longstanding territorial-cultural rivalries and tensions. So whilst risk management for the Olympics tends to concern protection of critical infrastructures and trans-national coordination and exchange of intelligence concerning specific threats, for football World Cups and European Championships this tends to be focused upon maintenance of public order and effective crowd management, often with a distinct national flavour to policing styles (albeit with the exchange of some intelligence between national agencies and support from specialist units). Thus, the Olympics involve surveillance of a different kind to that of international football tournaments (attempting to anticipate, detect and avert prospective attacks by individuals or groups), whereas the latter are predominantly managed as a public order concern that is reliant upon policing at street-level, supported by cooperation between national police forces.[23]

The security risks that confront sporting mega-events are therefore diverse, complex, and often context-specific. While this multitude of potential sources of disruption might give rise to a fatalistic outlook of the prospects of managing security risks, there remains a need to address these risks one way or another. What security risk management tools are in the governmental toolbox in the planning of mega-events when comparing the 2012 Olympics with the 2006 Football World Cup in Germany?

Comparing security risk management tools

Comparing security risk management of different mega-events in two countries invites a criticism of comparing apples and oranges. However, as noted above, both of these are clearly sporting mega-events (they are both fruit – we are not comparing apples with lions), and, if the arguments regarding isomorphism are correct, then some degree of cross-reading across these mega-events should be expected. Direct comparison between these events is complicated at the present time because one event has occurred – successfully, with disturbances only recorded in the context of three matches (Poland-Germany, England-Sweden and England-Ecuador), and three streaking incidents ('Flitzer') also noted – and was replicated by the organisers of the UEFA 2008 European Football Championships, whereas the security risk management tools for the London 2012 Olympics are still in a state of evolution, though for the most part adheres to the general template of security arrangements at previous Olympics. Nevertheless, the cases provide a basis for refining the tools of government approach for analysis of different modes of risk management and for diagnosing general characteristics of management of security risks at sporting mega-events.

Nodality

[23] Of course, football world cups are also treated as potential targets for threats associated here with those of the Olympics. We are making a point regarding emphasis.

Copyright PSA 2009

As noted, nodality tools seek to extract and utilise information for the achievement of particular objectives. Most notable across the two mega-events was the use of nodality for the detection of particular security threats, in particular by locking the local event(s) into the wider information exchange across national and international police forces.

In the case of the 2006 World Cup, Germany built upon bilateral agreements with thirty-six other countries. These mechanisms had already been utilised in previous European tournaments as well as at the Athens 2004 Olympics. As such, the security risk management strategy utilised ongoing and existing information flows that had already started to focus on particular fan groups (i.e. hooligans). As central nodal point, the German federal government operated a 'National Information and Cooperation Centre' (NICC) to collect and summarise information and to disseminate it across the various locations in which the tournament was taking place.[24] Other nodality mechanisms operated to survey and manage road traffic flows (the 'SOCCER transport research project'), more importantly, accreditation and ticketing were utilised to inform security measures and to steer traffic flows (for example, tickets not only provided for access to matches, but also to public transport and contained information regarding road access to stadiums).

In staging of the Olympics, high-level security arrangements tend to be super-imposed over existing national and international infrastructures of intelligence exchange and defence capacities, albeit dependent upon the sometimes unique geopolitical context (i.e. the Beijing 2008 Olympic Games involved less formal/direct international cooperation on intelligence matters than Athens 2004). For London 2012, existing intelligence agencies (such as the Joint Intelligence Committee, MI5, MI6, 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.

In addition to this UK-specific coordination, there are also transnational arrangements for intelligence gathering. For each Olympics since Atlanta 1996, organizers have 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 a hundred countries and international organisations. Whereas football tournaments tend to adhere to a relatively hierarchical structure of intelligence analysis, there are multiple centres in the Olympic governance of security risks. This creates a greater capacity for information gathering and a more diverse set of intelligence sources, but at the same time adds 'noise' to the information signal that reaches analysts. This difference reflects, at least in part, the relative asymmetry of the types of security threats faced by Olympic and World Cup or European Championship organizers.

Authority

As noted, authority relates to tools that build on the force of legal authority, such as licensing, prohibitions and other type of orders. The exercise of authority is essential to security arrangements at both the Olympics and Football World Cups. The organising committees for both type of events are usually established as 'private law companies' and associations (e.g. the German Football Association (DFB)), operating, however, with the

[24] See http://wm2006.deutschland.de/EN/Content/SharedDocs/Downloads/seventh-progress-report-fifa-world-cup,property=publicationFile.pdf . (overview: http://wm2006.deutschland.de/EN/Content/SharedDocs/Downloads/)These arrangements were arguably less problematic to set up than those that were attempted in the case of the earlier world cup staged jointly in South Korea and Japan.

Copyright PSA 2009

support of public agencies (at various levels of government) for the provision of infrastructure, security and other essential services.[25] In the German case, the use of authority is particularly problematic as security is mostly an issue of the state level. As a result, security risk management was largely managed through a wider political-intergovernmental process in which the lead ministry, the federal ministry of the interior, developed the agenda in agreement with the interior ministries of the Länder. The only aspect in which the federal level was fee to utilise its legal authority was in re-instating border controls and thereby being able to reject entry to particular individuals associated with security risks (i.e. hooligans). In addition, stadiums were often in private-law hands, further complicating the ability to steer hierarchically through law. Public viewing events were 'steered' through licensing and other security standards. However, especially the areas of security, was dominated by negotiated solutions within the intergovernmental process, as well as in the network of emergency responders, headed by a federal agency, the Technisches Hilfswerk (see below).[26]

Given that the world cup involved the use of existing stadium infrastructures, there was a substantial contrast to the type of legal authority required for planning purposes that had to be utilised for the 2012 Olympics. Nevertheless, stadium modernisation (as organised through the private or municipal owners of the stadiums, with the exceptions of Berlin and Leipzig) followed the international standards in terms of stadium safety and access.

The special legal framework enacted for staging the London 2012 Olympic Games does not correspond to the powers of those government agencies responsible for securing the Games. While infrastructure and venues are to be constructed by the Olympic Delivery Authority (ODA), established under the *London Olympic Games and Paralympic Games Act 2006*,[27] and the events are to be operated by the London Organizing Committee for the Olympic Games (LOCOG), a private company owned by the government, security for the Games entails a complex network of public and private organisations that intrudes upon multiple jurisdictions, responsibilities and legal powers. While the various police, security and emergency services for the London 2012 Olympics operate within particular jurisdictions, they are coordinated through a single Olympic command structure.[28] This is typical of the traditional hierarchical, state-dominated character of the Westminster system: where central government is responsible for securing London 2012 despite the lead role of LOCOG in staging the Games and the ODA in delivering the main venues. The ODA and LOCOG retain certain authorities over integration of security in design of infrastructure and stadia, and protocols or technologies such as ticketing and on-site checks. However, the Cabinet-level Olympic Security Committee, chaired by the Home Secretary and consisting of representatives of UK security and resilience agencies, is the ultimate authority concerning security matters and inter-agency coordination. At the same time, the Commissioner of the Metropolitan Police is responsible for planning and operational matters that concern terrorism and policing in London. While the police and MI5 report to the Home Secretary, MI6 reports to the Foreign Secretary and the armed forces report to the Defence Secretary. As such, political authority over security organization for London 2012 rests at cabinet-level and comes with pre-existing legal and institutional capabilities and powers.

[25] We are not considering here the use of legal authority to suspend work permit, working hour or customs clearance regulations.

[26] Apart from the federal complication, there was a further inherent tension (termed a 'highly delicate form of co-operation' by in terms of the ownership of the world cup, with the international football association's (FIFA) legal contracts taking priority over those signed by the German association. However, this highly delicate form of co-operation mainly concerned issues of sponsorship rather than the provision of security risk management measures.

[27] London Olympic Games and Paralympic Games Act 2006.

[28] See London 2012 bid.

Copyright PSA 2009

Organisation

The tool of 'organisation' reflects the physical presence of the state in intervening directly in security risk management, this can either occur through the use of 'security' forces, the utilisation of emergency support and through the use of architecture more broadly.

In the case of the football world cup, all these three mechanisms were utilised to a considerable extent, requiring however extensive intergovernmental co-ordination processes.[29] In terms of policing (and linked to the tools of nodality as brought together through NICC). In the case of policing, the main 'safety' framework was co-ordinated through a 'Stab' in the federal ministry of the interior that however operated through the normal operating procedures of federal-Land co-operation (the standing committee of interior ministers). A sub-committee dealt with the particular issue of policing and crime, thereby accessing directly tools of nodality. However, in addition, it utilised close co-operation with other national police force: 570 foreign police were active in Germany to monitor fans and inform German security forces.

In terms of non-policing security measures, the Länder were solely responsible for fire brigade, rescue and emergency services. However, the overall co-ordination operated through two federal agencies, the Technisches Hilfswerk, which was largely in control of emergency services, in particular in terms of infrastructures (communications, electricity), and the Bundesanstalt für Bevölkerungsschutz und Katastrophenhilfe which provided extra equipment as well as training for local emergency services. The army was also utilised to provide medical services (as well as providing a background 'policing role' which however was not called upon).

But 'organisation' was not just a matter of personnel, but was also provided through stadium architecture and the careful planning of transport access routes (again providing for a strong link to nodality). A crucial difference to events such as the Olympics was not just that the stadiums were regularly used for football matches, but that the running of the so-called Confederations Cup also provided for insights into potential security risks (a report that has not been published).

For the London 2012 Olympics, the network of organisations and manpower involved in security operations is complex and extensive. With high-level coordination from the Cabinet-level Olympic Security Committee, a range of government agencies will deploy their organisational resources with respect to certain tasks. MI5 and other intelligence services are to gather, disseminate and advice on intelligence matters, the Metropolitan Police and regional police forces are to provide policing, law enforcement and emergency responses (possibly with support from the armed forces), and the London Resilience Team[30] are responsible for contingency and consequence management planning, such as the London mass fatality plan.[31]

The demands of a considerable security presence can strain the resources of Olympic organizers. At Athens 2004, heightened security concerns after the events of September 11th meant that there were around 70,000 police on patrol in Athens and at the Olympic venues, necessitating external support in terms of presence from NATO as well as the European Union. At up to 14,800, the projected number of police for the London 2012 Games is far lower (with additional support from 6,500 private security contractors),[32] reflecting its reliance

---

[29] http://www.bmi.bund.de/cae/servlet/contentblob/139756/publicationFile/15274/WM2006_Abschlussbericht_der_Bundesregierung.pdf

[30] http://www.londonprepared.gov.uk/

[31] London Mass Fatality Plan, http://www.londonprepared.gov.uk/downloads/LMFPMainBodyV2.pdf

[32] London bid. Chapter 12, p.39.

Copyright PSA 2009

upon intelligence-gathering and processing instead of policing for Olympics compared with international football tournaments. That number is not insignificant, however, since it represents about 10% of the total UK police resource.

Organisation also refers to the set of event features that, like transport, determines the physical spacing, timing and structure of crowd flows and security provisions, as well as facilitating control and responsiveness in the case of incidents. For example, there is an increasing 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 familiarisation with peculiarities of each location, such as in relation to exit routes, evacuation plans and so forth. There is also a high degree of standardization of event schedules for sports events such as World Cups and Olympics, through guidance of international organizations such as FIFA and the IOC. The Olympic Village to house all athletes and support staff at London 2012 is to be located within the Olympic Park area, creating a general perimeter that requires securing (although there will be different levels of security within the Olympic Park). As most of the blue-ribbon events are to take place in the Park – at the main stadium and aquatics centre – this leads to a concentration of security efforts at a single site. However, in contrast to the enclosed architecture of football stadia, the main Olympic site tends to be more open and less structured in design (consisting of multiple venues, open spaces and interchanges). Whilst it still requires policing of its perimeter to manage security threats (in particular near the site entrances), there is a greater emphasis upon randomized and 'intelligent' surveillance inside the site. This means security presence tends to be less concentrated and, therefore, less visible. So whilst breaches of the secure perimeter in football stadia are more transparent to onlookers, the multi-centred layout of the Olympic site presents a more complex challenge for mobilizing intelligence and presence for the purposes of security.

The tool of organisation also takes the form of direct technological devices and controls used by government, often intersecting with intelligence-based strategies. Indeed, the Metropolitan Police have said that the 'first line' of Olympic security for London 2012 is the installation of a 'technological footprint' across London, such as CCTV, smart ticketing and automatic ID-recognition for both people and vehicles.[33] The ODA has sought tenders for the main Olympic site for a 'Command and Perimeter Security System' consisting of security lighting; intruder detection, access control and alarm systems; automatic number plate recognition; a command, control and communication infrastructure (C3i) integrated system; data network equipment; and associated security systems, information and communication technology and accommodation. The plans for 2012 also involve pedestrian screening areas (with an airport style security check of the person and any bags or equipment) and vehicle checkpoints to control the flow of authorized vehicles. Security scanners at the entrance to public transport or competition venues provide off-site and on-site turnstiles that provide a control on visitors and ticket-holders that are intended to filter out threats and disrupt black markets in ticketing.

Treasure

As noted, treasure is defined by the use of 'fungible chattels' to steer behaviour. In the case of the German football world cup, it is difficult to come to any form of estimate as to expenditures that were specifically invested into security risk management, as responsibility was, as noted, diffused between levels of government and between private and public parties. Federal investment in transport infrastructure was made independent of the world cup (estimated to be €3.7bn), there was some support for the modernisation of two stadiums (Berlin and Leipzig, nearly €250m), while the full economic cost for the use of the Bundeswehr

[33] Metropolitan Police Assistant Commissioner Tarique Ghaffur, quoted on BBC Online (10 April 2008) 'Torch lessons for 2012 Olympic security' (http://news.bbc.co.uk/1/hi/business/7340174.stm).

Copyright PSA 2009

was estimated to have been about €4.4. Other measures, such as the use of the federal police were budgeted through normal budget lines, while the use of NATO reconnaissance flights was paid for through the NATO budget (as had been the case with the 2004 Olympics and European championships). Indeed, the financial risk of the overall event was with the organising committee, and therefore lay purely with the German football association. The federal government did not play the role as lender of last resort. The overall event provided for a substantial profit for the German football association.

For the London 2012 Olympics, treasure is constituted both in direct expenditure by public bodies (e.g. ODA) and expenditure by private or quasi-private organisations (e.g. LOCOG) on public goods (e.g. security) funded through commercial activities such as ticket sales and sponsorship. The overall security budget is the responsibility of government, with the exception of security for the Olympic site in the Lea Valley. The latter, a fraction of the total, is to be funded through LOCOG's revenue from tickets, sponsorship and merchandise. The burgeoning budget for Olympic security in 2012 illustrates how financing of security management is a significant concern for the organizers of sporting mega-events. The initial feasibility study for a London bid included a "provisional sum for the cost of all security for the Olympics following consultation with the Metropolitan Police and based on the experience of Sydney 2000 and Salt Lake City 2002",[34] at a cost of £160.2 million.[35] ARUP reported that "with more time to plan security for a 2012 Games, the costs are not likely to reach those incurred at Salt Lake City [£245 million]".[36] Site security was costed at £190 million in the bid, increased to £268 million in the revised March 2007 budget which put the total/wider security and policing cost at £600 million.[37] Since then, security costs have been reported to reach £1.5 billion.[38] The public costs associated with securing the Games are a contested topic. In part this is because the Games are a national defence issue, and is not easily disbursed to the host OCOG or metropolitan government. The fixed costs of policing, intelligence and defence manpower might remain relatively stable, although these are diverted to the Games for a concentrated period of time. Furthermore, while comparison between different Olympics is a difficult business, it is evident that the cost of security at the Olympics has grown over the past thirty years, and dramatically since Sydney 2000 – with the events of 9/11. [39] An interesting observation is that in some political contexts, such as Beijing 2008, the lack of transparency over the actual security budget disguises the brute strength of the security provisions. Treasure tools for London 2012 also entail use of private contractors with responsibilities for security controls at Olympic venues, provision of spectator services staff, and operation of access control and 'mag-and-bag' (magnetometer and baggage) searches.

An alternative form of treasure that is used to insure against the effects of security risks is insurance. Prior to the events of 9/11, Salt Lake City 2002 took out cancellation cover with Lloyd's of London. Since then, insurance premiums for sporting mega-events have risen sharply as projected security risks have proliferated. For the first time, for Athens 2004, the IOC purchased $170 million cover for cancellation insurance to protect against financial losses of cancellation due to terrorism or natural disaster (with the premium reported to approximate $6.8 million).[40] This rose to $415 million cover for Beijing 2008, at reported premium of $9.4

[34] ARUP. (2002). Executive Summary, pp. 3-4
[35] ARUP. (2002). (Department of Culture, Media and Sport, Freedom of Information Request), p. 98.
[36] ARUP. (2002). (Department of Culture, Media and Sport, Freedom of Information Request), p. 95.
[37] House of Commons, Public Accounts Committee. (2008). The budget for the London 2012 Olympic and Paralympic Games. Fourteenth Report of Session 2007–08. London. The Stationery Office Limited. p. 9.
[38] Matthew Beard. (29 September 2008). "Security costs 'will send 2012 bill over £10bn'", Evening Standard
[39] See Wall Street Journal, 22 August 2004.
[40] Graham Buck, "Vaulting Olympic risk", Risk & Insurance (August, 2004), available at http://findarticles.com/p/articles/mi_m0BJK/is_9_15/ai_n6156490.

Copyright PSA 2009

million,[41] and can be expected to rise again for London 2012. As such, treasure mechanisms are used to protect against security risks that also pose treasure risks (in terms of the financial viability of the Games). Thus, insurance functions as a form of asset protection and remediation, instead of security functions that attempt to deter and inhibit attacks or disruptions.

Table 3: Tools of security risk management at the London 2012 Olympics and the FIFA 2006 World Cup in Germany

Treasure	**Nodality**
Olympics Public-private expenditure Insurance cover Private security contractors Defence expenditure	Intelligence (e.g. Olympic Security Committee) Counter-terrorism Transnational information-sharing Olympic Intelligence Centre Risk assessments Knowledge transfer programmes
World Cup Public-private expenditure German Football Association NATO funding of reconnaissance	World Cup National Information and Cooperation Centre Bilateral agreements Hooligan databases Transnational exchange of information Crowd 'spotters'
Organisation	**Authority**
Olympics Layout/architecture of the Olympic site Police Emergency services CCTV monitoring Pedestrian screening	Olympics Special legal protection (i.e. Olympics Act) Private operating company Central government (unitary system) International governance (IOC) Cabinet-level coordination of strategy
World Cup Stadium design and access routes Police Emergency services Foreign police Fan miles CCTV monitoring	World Cup Private operating company Federal-state government Immigration controls International governance (FIFA) Licensing Ticket controls

Conclusion

What insights has this analysis offered on the risk profile of the London 2012 Olympics and FIFA 2006 World Cup in Germany and different approaches to security risk management at these mega-events? How might this help diagnose general characteristics of management of security risks at sporting mega-events? This analysis has provided an evidential basis to start to resolve such questions: establishing similarities and differences in the risk profiles of Olympics and football World Cups, identifying the specific tools of risk management used in these cases, and diagnosing the various trade-offs and side effects of generic categories of risk management tools at sporting mega-events.

[41] Dave Lenckus, 28 July 2008, 'Beijing 2008 Olympics cancellation cover led in Europe', Business Insurance.

Copyright PSA 2009

First, it has been established that sporting mega-events such as Olympics and football World Cups are high risk and vulnerable to crisis situations for several reasons. The global profile of events and international competition makes them a target for terrorism, eruption of geo-political or nationalist tensions and other critical incidents. Even without such threats, the staging of a mega-event is susceptible to organisational or operational failures – because of its scale and scope – that can result in second order failures (i.e. 'normal accidents'). At the same time there are clear differences in the specific risk profiles of Olympic Games and World Cups, even though these share numerous organisational features. The Olympics tends to be at risk of terrorist attacks and system failures, such as for infrastructure or transport networks, whereas World Cups are more prone to problems with public disorder concentrated at specific locations or venues.

Second, using the NATO framework this analysis has identified different modes of risk management used at the London 2012 Olympics and the FIFA 2006 World Cup in Germany, in the form of nodality, authority, treasure and organisation. Each of the cases is characterised by the relative heterogeneity of its toolkit of security risk management, with no single approach dominant over all the others. The tools used for Olympics and World Cups are consistent with functional requirements and specific risk profile of each-mega event, consistent with theoretical expectation of differentiation. This finding also highlights methodological difficulties involved in generalisations about governance of sporting mega-events subject to distinct organisational features and unique risk profiles. However, this does not mean that there is clear evidence for a rejection of the 'institutional isomorphism' hypothesis, but similar tools are largely taken from successor events (i.e. in the case of football world cups from European football championships). Furthermore, how particular tools are being utilised depends not just on the particular risk profile of an event, but also on the wider political system. For example, the importance of negotiated co-ordination (with only a limited possibility of a shadow of hierarchy) was a critical aspect of the German experience and shaped the extent and character of the respective tools that were utilised.

Third, selection and use of specific tools of security risk management at mega-events is associated with corresponding trade-offs and side effects. Treasure is associated with problems of forecasting effects and costs/revenues at one-off events. This is manifested in the recurring problem of predicting and controlling the public expense of mega-events (such as the Olympic cost-overruns at Montreal 1976, Sydney 2000, Athens 2004, and London 2012). The resource commitment required to secure a mega-event is vulnerable to both supply and demand-side changes in the wider political and economic environment. For example, the events of 9/11 led to an unanticipated increase in expense of security provisions for the Athens 2004 Olympics. Likewise, a £600 million provision for security at London 2012 is now far more problematic, in both political and financial terms, in the context of the global financial crisis. Thus, external factors can exert considerable strain upon resources available for management of security risks. Treasure also appears to be strongly correlated with political control, i.e. authority, inasmuch as government has a direct role in the financing of security tools. This is, furthermore, at odds with nodality since it creates a bias towards centralised and hierarchical forms of security risk management, i.e. direct force. Organisation, has the potential characteristic of being something of a sledgehammer to crack a nut, again in contrast to intelligence-based approaches, although street-level surveillance is, it should be noted, an integral prerequisite for nodality. Deployment of a large armed or unarmed security presence can cast a shadow over staging of a mega-event, undermining the conviviality of the occasion for both competitors and spectators. The success of the 2006 World Cup operation is, in part, attributable to its non-intrusive security presence (as part of a wider attempt to reform policing and its image). Organisation combines logics of deterrence, prevention and reaction, although it is conceivable that the concentration of security at a particular site or at critical nodes in the infrastructure network might lead to

Copyright PSA 2009

attacks on the periphery rather than the centre. This might also result in partial redundancy of nodality, with a large presence of security forces on the ground crowding out the usefulness of onsite intelligence. This tool remains vulnerable to the problem of isolated attackers that manage to slip through the net, however.

Authority is a pervasive, and often invisible, feature of security management at sporting mega-events – in establishment of funding and delivery structures, definition of organisational jurisdictions, and granting power to security services to monitor, control or detain individuals. While authority empowers treasure, organisation and nodality, hard-wiring of legal provisions can, inadvertently, create future inflexibilities in response to incidents or create competition or conflict between different organisations. The fragmentation of legal authority and jurisdictions can itself give rise to blind-spots in management of security risks. For example, the complex network of domestic and international intelligence agencies involved in securing the London 2012 Olympics is vulnerable to excessive noise from multiple information signals, and danger of information not being shared between organisations, such as in the intelligence failings prior to 9/11.[42] For the football World Cup, legal restrictions are most prominent in the context of managing public order so, therefore, are not as problematic. While legal authority is, therefore, a function of the specific risk profile of the mega-event, its use as a tool of risk management is also dependent upon the national political system. For the London 2012 Olympics, the unitary parliamentary system of government is associated with centralised coordination of security arrangements as well as reliance upon street-level deployment of public services (organisation). The federal system in Germany resulted in a more collaborative and networked approach (nodality) for the 2006 World Cup. The institutional context therefore can be associated with selection of certain tools, though the evidence is tentative at this stage.

Last, nodality is vulnerable to the problem of 'group think'[43] in intelligence sharing and risk assessments. This remains an important counter-balance to organisation, however, since it provides a basis for optimal deployment of attention and security forces. Perversely, the silent and clandestine characteristics of nodality in the mysterious world of spooks and intelligence means that it struggles to inspire public confidence, creating ambiguity over the degree to which security risks are being managed. There is, furthermore, tension between authority and nodality tools, because organisational jurisdictions can create barriers to intelligence sharing and dispute over 'ownership' of particular security risks. For sporting mega-events, the relative lack of visibility of nodality makes it something of the odd man out, yet is perhaps the most critical tool – certainly as far as management of Olympic security risks is concerned. While the public order aspects of football tournaments tend to require greater emphasis on treasure and organisation.

Overall, comparison of tools of risk management provides evidence of fragmentation and isomorphism, though this requires further investigation. The tools used for Olympics and World Cups reflect functional differences in these cases as well as the high risk nature of mega-events. There are also similarities, however, in use of a diverse toolkit of approaches to security risk management and diffusion in practices between Olympics and between World Cups, with replication of institutional structures. As such this analysis has illustrated the usefulness of the NATO approach to categorisation of management of security risks at sporting mega-events. While there should be caution in generalisation about mega-events, a generic categorisation of forms of risk management can provide insight on the problems and solutions that are present in organisation of the world's major sporting events.

---

[42] 9/11 Commission (2004) Final Report of the National Commission on Terrorist Attacks Upon the United States (http://www.gpoaccess.gov/911/index.html, last accessed 16 June 2008).
[43] Janis, Irving L. (1972) Victims of Groupthink, Boston, Houghton Mifflin Company.

Copyright PSA 2009