carr
centre for analysis
of risk and regulation

centre for analysis
of risk and regulation
An ESRC Research Centre

Tools of Security Risk Management for the London 2012 Olympic Games and FIFA 2006 World Cup in Germany

Will Jennings and Martin Lodge

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

DISCUSSION PAPER NO: **55**
DATE: **November 2009**

Tools of Security Risk Management for the London 2012 Olympic Games and FIFA 2006 World Cup in Germany

Will Jennings and Martin Lodge

Contents

The work was part of the programme of the ESCRC Centre for Analysis of Risk and Regulation.

Published by the Centre for Analysis of Risk and Regulation at the

London School of Economics and Political Science

Houghton Street

London WC2A 2AE

UK

ISBN 978-0-85328-397-3

Printed and bound by Kube, November 2009

Tools of Security Risk Management for the London 2012 Olympic Games and FIFA 2006 World Cup in Germany

Will Jennings and Martin Lodge[1]

Abstract

Mega-events such as the Olympic Games and the football World Cup represent a special venue for the practice of risk management. This paper explores management of security risks in the case of two sporting mega-events, the London 2012 Olympic Games and the FIFA 2006 World Cup in Germany. The analysis progresses in three stages. First, it explores three explanations that have dominated the literature on policy instruments and tools and introduces the generic tools of government approach developed by Christopher Hood (1983). Second, it reviews the tools used for security risk management at the two mega-events. Third, it evaluates competing explanations of tool choice and degree to which these are consistent with organisational strategies of risk management at the events. The findings highlight the importance of national political systems in influencing tool choice.

Acknowledgements

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'.

[1] Authors are listed in alphabetical order.

Introduction

Moments of crisis and the handling of post-crisis moments have attracted increased attention across the social sciences in recent years, in a large part as a result of focusing events such as 9/11, the Asian Tsunami or Hurricane Katrina. The public and private management of risk has likewise been subject to extensive analysis (Boin et al. 2005, 2008; Hood et al. 2001; Power 2004, 2007; Rosenthal et al. 1989). Mega-events, defined as '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' (Roche 1994: 1), are an important case for analysis of the management of security risks. They combine both scale and scope with substantial interdependencies, resource commitments and geopolitical significance under the watchful eye of the international media and publics.

While literatures in public management and organisational theory have taken an increasing interest in the governance of risks and crises, studies of public policy have seen a return to analysis of policy instruments and tools. This follows an earlier period in the 1980s when different sets of typologies and approaches were applied to understand the means through which governments sought to affect and govern their populations (Linder and Peters 1989: 35-38). The current analytical revival revisits these original approaches, and considers the extent to which two decades of change and reform – in particular in information technology but also in other socio-economic and political dimensions – have impacted upon the nature of the tools of government and how the tool mix has changed across policy domains and states (Hood 2007: 127-44; Lascoumes and Le Gales 2007: 1-21; Salomon 2002).

This paper integrates insights from these public administration literatures to provide a distinct perspective on risk management. Most analyses of risk management trace decision-making processes, highlight organisational or operational failures, or advocate certain solutions or improvements to risk management strategies. This paper instead analyses determinants of tool choice. In other words, it attempts to improve understanding of the logic of choice of approaches to risk management at mega-events. It concentrates upon the case of two sports related mega-events: the FIFA 2006 Football World Cup in Germany and preparations for the London 2012 Olympic Games. The analysis also contributes insights on governance of mega-events, World Cups and the Olympic Games (Altshuler and David Luberoff 2003; Flyvbjerg et al. 2002: 279-95, 2003; Hall 1989: 263-68).

This paper is organised in four parts. Firstly, it explores three explanations of tool choice – isomorphism, functional/differentiated responses, and national political styles. Secondly, it introduces the tool approach to analysis of security risk management, borrowing from Christopher Hood's 'NATO' (nodality, authority, treasure, and organisation) classification system of policy instruments and tools. Thirdly, it applies this toolbox approach to the case of security plans and operations for the 2006 Football World Cup and the London 2012 Olympics. The analysis of this

pair of events maximises leverage for possible insight: Germany and the UK are developed and liberal-democratic European countries that are characterised by differences in political institutional framework. While one event is in the past and the other in the future, the focus of analysis is the form and choice of tools of risk management rather than the success or failure of these strategies. This also enables insight into the diffusion or isomorphism of tools. Finally, the paper concludes with an assessment of the relative power of the three explanations in light of observed patterns of tool choice and considers the wider implications for analysis of policy tools (or instruments) and for risk management of security risks in particular.

Tools for the job: different logics of tool choice

Three explanations of why decision-makers choose particular policy tools rather than others (though these are neither exhaustive nor mutually exclusive) are prominent in the wider public policy literature (Lodge 2007: 277-79). Each of these logics is relevant for the analysis of mega-events, such as the Olympic Games or the football World Cup. In this section, these logics of tool choice are introduced along with the potential implications of tool choice for comparison of the particular types of mega-event. This enables formulation of distinct expectations of the observable implications for the empirical analysis that follows. In the wider sense, this analysis also contributes to debates as to what determines policy tool choice.

Tool choice as institutional isomorphism

What makes tools of risk management so similar across different political and organisational contexts? In their influential analysis, DiMaggio and Powell (1991: 66) distinguish between three sources of institutional isomorphism – that is processes of appropriateness and legitimisation that cause organisations operating in the same environment to increasingly resemble one another, rather than to behave according to principles of survival of the fittest in a process of natural selection. These sources are *coercive* (existence of a central source that prescribes particular organisational responses), *mimetic* (copying or mimicking of recipes that appear legitimate or successful) and *professional* (existence of a dominant professional set of doctrines about how to organise).[2]

There are reasons to suspect that isomorphism is a potential influence upon the governance of risk in mega-events. First of all, planning and operational decisions at mega-events are taken under conditions of high uncertainty and high tension, subject to high search costs, encouraging searches for organisational strategies that are perceived to be legitimate or successful. These particular sporting mega-events are similar in their exposure to optimism bias during the award and planning stages and to risk aversion in the later operational stages, each of which both distort tool selection in favour of existing norms, protocols and standards (Jennings and Lodge forthcoming). The competitive process for awarding the right to host once-in-a-

[2] DiMaggio and Powell call the third mechanism ‘normative’.

generation events such as the Olympics or the World Cup encourage unrealistic or over-optimistic bids, drawing upon the bid templates or assumptions from past bids and utilising pre-existing communities of knowledge and practice.

This process of institutional isomorphism therefore offers a convenient solution to the 'impossible job' (Boin and 't Hart 2003: 544-53; Hargrove and Glidewell 1990) of organising mega-events. Such events entail numerous uncertainties concerning the prioritisation of specific risks, the selection of particular indicators to monitor and evaluate information about risks, and use of certain policies and organisational instruments to mitigate certain threats or hazards and modify behaviour (Jones and Baumgartner 2005).[3] While risk management in all its forms is required to balance different priorities, mega-events represent a special test due to their exceptional scale and complex nature. This is further aggravated by the rotation of event locations at the instruction of international authorities, restricting the pool of existing knowledge and expertise to a small community of experts, all of which again might be expected to lead to greater isomorphism. Most of all, combination of the public/media spectacle of mega-events with the synoptic and controlling aspirations of the regulatory state generate conditions that somewhat resemble Perrow's claim that particular industries are confronted with tragic choices in their vulnerability to 'normal accidents' (Perrow 1999). Demands for decentralised co-ordination of risk management have to be combined with conflicting demands for synoptic and centralised control (Moran 2001).

In addition, mega-events are global phenomena often attracting a worldwide television audience of billions, millions of spectators and wide-ranging public and media interest. In front of that kind of audience, decision-makers have little room for things to go wrong and little scope for adapting in response to external attacks or system failures. Opening ceremonies, competition schedules and venues are often fixed years in advance, creating added pressure for things to be 'alright on the night' and dependence upon conventional wisdom and protocol to deflect criticism. This setting increases the opportunities for rent-seeking. For example, essential workers in public services or project delivery acquire increased negotiating leverage through strike threats, while security professionals emphasise certain risks that need to be mitigated. The global dimension of mega-events also accentuates isomorphism of threats and hazards (in addition to the tools of risk management). This creates a platform for the airing of grievances or agendas where certain groups or individuals (e.g. anarchists, anti-globalisation protesters and terrorists) advertise their intentions to interrupt staging of the event, while other threats consist of intelligence chatter. Thus, management of security risks is confronted with the choice of which of these mimicked risks to discount, which to monitor, and which to mitigate and protect against.

The rise of a risk management consultocracy since the 1980s (Power 2004) might also be expected to contribute to growth in the transfer of risk management tools across

[3] This is subject to the same general kinds of cognitive and institutional biases ('friction') of attention identified in the model of disproportionate information processing.

international boundaries and across sporting events. There are wider pressures, then, for professional institutional isomorphism in governance of risk at mega-events. This imitation would be manifested in the presence of dominant logics of appropriateness or administrative protocols in the application of risk management tools (March and Olsen 1989, 2009). It is possible to identify potential sources of coercive forms of institutional isomorphism in international guidance and requirements, such as the 2004 *EU Handbook* on securing against terrorist acts at major sporting events or the 1985 *European Convention on Spectator Violence at Sports Events* (this document responded to Heysel tragedy in Brussels and the long history of English football hooliganism). Likewise, within the Olympic movement there are International Olympic Committee (IOC) standards concerning bid documents and progress monitoring by the IOC's Evaluation and Coordination Commissions.

Tool choice as a functional response to specific risk profiles

In contrast to expectation of similar responses in security risk management tools, an alternative view of tool choice is of a response that reflects the particular attributes and the risk profile of the mega-event in question. Studies of regulation would characterise this explanation as a response of risk management to a specified diagnosis of market failure. Thus, tools are chosen depending on functional requirements of the particular event, as governments seek to economise their resource use. This logic suggests that decision-makers select their tools based upon careful and systematic gathering of information, an assessment of the target population, and comprehensive assessment of desired safety or security standards.

Considerable variations can be identified in the organisational format of mega-events as well as in their exposure to risks and threats. Accordingly, these differences should be expected to matter in choice of tools of risk management. For example, international football tournaments tend to be associated with problems of public disorder, violence and organised hooliganism, with large crowds of national (and sometimes local) supporters congregating in or around urban centres for specific matches. This contrasts with spectators at the Olympic Games which tend to consist of a more diverse mix of local and transnational audiences that do not support athletes or teams in such a partisan and nationalist fashion. While both the Olympics and football World Cups are potential platforms for political demonstrations or terrorist attacks, such threats are more prominent in the case of the Olympics, with historical precedents such as riots prior to Mexico City 1968, the 1972 Munich Massacre, and the 1996 bombing of Centennial Park in Atlanta. The form of security conflicts and threats at these mega-events therefore tend to be realised in quite different forms.

There are further differences in the organisational scale and complexity of events. The London 2012 Olympics 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 the 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 security task is of a different order from organisation to the FIFA 2006 World Cup in Germany which consisted of some 64 matches involving 32 teams played in 12 stadiums in 12 different cities over a month of competition with 52,000 spectators on average per match (3.3 million in total).

Another difference is location. International football tournaments tend to be decentralised to multiple regions, towns and stadia, reducing the likelihood that a critical breakdown or security incident in one location will cause a system-wide disruption. At the Olympics, a significant proportion of events are held at specialist venues on or near the main site (which for recent Games has consisted of the athletics stadium, aquatics centre and the athletes' village). The technical requirements of competition venues are a significant determinant of the critical impact of security incidents in forcing interruption or abandonment of the event. While there are in the region of 40 football grounds in the UK with capacity for somewhere between 20,000 and 40,000 spectators there are just two Olympic-standard swimming pools and no international standard athletics stadium (with the abandonment of the Picketts Lock project and conversion of the City of Manchester stadium for use as a football stadium after the 2002 Commonwealth Games).

A one-off disturbance of security – whether technological, natural, or man-made in origin – therefore has the capacity to disturb the staging of an Olympics far 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 one central venue makes the symbolic and reputational effects of breakdowns in security all the more powerful – although such effects would also be noticeable if an incident occurred during opening and final matches of the football tournament. Indeed a power outage during the Euro 2008 semi-final between Germany and Turkey interrupted transmission of the feed to television broadcasters and generated a PR problem for organisers.

At international football tournaments, relative decentralisation of each of the games causes spectators to descend upon locations for a concentrated period of time. This means 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 new risks into management of transport hubs and links. Given the recent fashion for public viewings on giant television screens in town centres and official licensing of public overflow zones for events (e.g. fan miles), additional security is often required to cope with the unpredictable numbers of spectators outside stadiums and in nearby urban centres or districts. This places a further strain upon policing and emergency services. As witnessed in the 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 more than 150,000 supporters meant that local restaurants ran out of food long before kick-off.

There are therefore important differences in the security uncertainties and threats that confront the organisers of sporting mega-events. For the case of the Olympics these tend to concern geopolitical conflict and domestic or international terrorism. For the case of football World Cups and other international football tournaments, large crowds of national supporters (sympathising with opposing teams) create security risks that are manifested in public disorder or violence and based upon longstanding territorial-cultural rivalries and tensions. While security risk management for the Olympic Games tends to concern protection of critical infrastructures and trans-national coordination of intelligence concerning specific terrorist 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.[4]

Unlike institutional isomorphism where decision-makers are assumed to utilise pre-existing solutions or strategies in the face of uncertainty and high search costs – conditions associated with bounded rationality (Simon 1957), the 'risk profile' approach predicts considerable differences in the utilisation of tools of security risk management.

Tool choice as a result of national political systems

Political institutions matter. This much is clear, but institutional design and jurisdictions determine the discretion of governments to select particular policies or tools (Levy and Spiller 1994: 201-46). The third logic of tool choice therefore refers to the effect of institutions on approaches to management of security risks. Comparative studies have noted the importance of policy styles and state traditions to government (Hall 1986; Richardson 1982). This logic suggests that political institutional frameworks lead to differences in tool choice, where this might be due to differences in state structure (federal vs. unitary states), engagement with private and para-public interests (pluralist vs. corporatist decision-making) or government formation (single-party vs. coalition government). Such variations in the institutional context are a potential source of differences in use of particular approaches to risk management.

Again, considerable differences in tool choice might be expected to emerge from this analysis given the substantial differences between the German and UK political

[4] 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.

systems. This contrast between cases applies both to distinction between consensus versus Westminster democracies (Lijphart 1999), and between the different 'varieties of capitalism' (Hall and Soskice 2001). Germany is governed through its system of executive federalism that requires a co-operative approach towards co-ordination of the different state police services (*Landespolizei*), for example. Likewise, its community of emergency services (first responders) is characterised by organisational diversity held together by a degree of shared norms and procedural understandings. The unitary state in the UK (in particular in England) might be expected to have strong effects upon tool choice, with competition between authorities representing London (including the London Mayor, London local boroughs and London-specific public agencies), and national departments and agencies along with Olympic organisations and the wider Olympic movement.

The mechanisms and observable implications of these different logics of tool choice are summarised in Table 1.

Table 1: Overview of logics of tool choice

Mechanism	**Observable Implication**
Risk profiles require different responses in terms of economising on tool depletion	Differences 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	
National political institutional endowment requires different responses given different resource and 'leverage' allocation across the political system	Differences in tool utilisation in security risk management

The toolbox: introducing the 'NATO' perspective

So how then compare the tools of risk management? This paper employs the classification scheme introduced by Christopher Hood (1983) almost three decades ago. Hood's theoretical framework offers a critical lens for the categorisation and analysis of different tools through which government interfaces with society, rooted in a cybernetic understanding of this relationship between the state and its citizens. This approach focuses on those *resources* available to policy-makers for gathering information and modifying the behaviour of its citizens. Hood distinguishes between

'effecting' and 'detecting' tools, i.e. those that seek to alter behaviour and those that seek to gather information. The government toolbox – of nodality, authority, treasure, and organisation ('NATO') – constructed by Hood and brought into the digital age by Hood and Margetts (2007) is outlined in Table 2.

This paper combines Hood's more generic perspective with assessment of determinants of tool choice, as advanced, for example, by Linder and Peters (1989: 35-58), Salomon (2002) and Hood (2007: 127-44). The focus on resources available to policy-makers is essential to Hood's toolbox approach, and is critical in identifying those patterns that might be predicted by explanations that focus on the effects on tool choice of risk profiles or institutional systems. In contrast, in a world where there are ambiguities concerning causes and effects and where resource implications are severe, it should be expected that legitimacy would be a chief resource in choice of tools, with decision-making processes oriented from the logic of appropriateness.

Table 2: The tools of government (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 authorisation 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 directly part of the government apparatus, but exist somewhere in the twilight zone between public and private sectors.

Lastly, *organisation* refers to the capacity of government for undertaking direct action, for example in its mobilisation 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. 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, 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.

Comparing security risk management tools

Comparing the security risk management tools of two mega-events in two countries invites the criticism of comparing apples with oranges. As noted above, however, both of these are clearly sporting mega-events (they are both fruit – analysis is not comparing apples with polar bears) and, if arguments regarding isomorphism are correct, then some degree of cross-reading across these events should be expected. Mega-events are, by definition, quite exceptional due to their bespoke organisational design, which encourages a false belief that general comparisons and lessons cannot be drawn. The objection that 'risk' and 'risk management' are words reserved for the Anglo-Saxon administrative space can also be rejected. The internal and external documents published for the FIFA 2006 World Cup (in German) and the local German 'security/emergency management' community endorsed the risk management approach (the official title was *Sicherheitsmanagement* – 'security management' – but

the approach was informed by Anglo-Saxon risk management language and methodology). Such a concern also points to a wider discussion as to what is meant by the term 'risk'. In this paper, risk is defined in its classic form and is used to identify incidents with potential to interrupt the running of a mega-event rather than as an organising principle that shapes the exercise of particular tool (a risk-based approach towards the employment of security personnel, for example).

The direct comparison of security at these events is further complicated because one has passed with minimal incident and the other is still in a state of planning and preparation. At the 2006 World Cup disturbances were only recorded in the context of three matches (Poland-Germany, England-Sweden and England-Ecuador). Three streaking incidents ('Flitzer') were also noted. Such a non-eventful outcome was replicated by the organisers of the UEFA 2008 European Football Championships (two 'Flitzer' incidents). In contrast, the management of security risks for the London 2012 Olympics is still in a state of evolution, although a clear organising template is in place. The purpose of analysis is to understand better the form and choice of tools of risk management rather than the success or failure of these strategies. Indeed, whether or not a security incident occurs at a given mega-event does not necessarily indicate the flaws in the logic of appropriateness or the particular risk management tool employed. There is such a thing as bad luck, even in the world of risk.

Nodality

As noted, nodality tools seek to extract and utilise information for the achievement of particular objectives. Most prominent across the two mega-events was the use of nodality for the *detection* of specific 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 36 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.[5] Other nodality mechanisms operated as effectors, in particular 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).

[5] 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.

In staging of the Olympics, high-level security arrangements tend to be superimposed 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 co-operation 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 organisations: 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, organisers 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 organisers.

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 and authority as a tool is prominent in particular as effector.

The organising committees for both types of events are usually established as private law companies and associations (e.g. the German Football Association [DFB]), operating, however, with the support of public agencies (at various levels of government) for the provision of infrastructure, security and other essential services.[6] In the German case, the use of authority as effector 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 politico-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 able 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.

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

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. 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).[7]

Given that the football 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 created a fragmented set of jurisdictions and responsibilities across the Olympic Delivery Authority (ODA), London Organising Committee for the Olympic Games (LOCOG) and Metropolitan Police (within the Home Office). Such an institutional framework is a potential source of ambiguity and tension over responsibilities for management of security risks associated with infrastructure and operations – with distinction between on-site and off-site risks and between pre-games and games-time risks. While infrastructure and venues are to be constructed by the ODA, established under the London Olympic Games and Paralympic Games Act 2006, and the events are to be operated by 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. For example, the allocation of legal responsibilities for delivery and operation means that those organisations responsible for security do not have formal access to the main site until the ODA hands it over (expected to be in 2011). Such divisions can trigger differences in risk prioritisation.

While the various police, security and emergency services for the London 2012 Olympics operate within particular jurisdictions, they are co-ordinated through a single Olympic command structure.[8] 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 stadiums, 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

[7] Apart from the federal complication, there was a further inherent tension (termed a 'highly delicate form of co-operation') 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.
[8] See London 2012 bid (2004).

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 organisation for London 2012 rests at cabinet level and comes with pre-existing legal and institutional capabilities and powers.

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/or through the use of architecture more broadly. As such organisation is utilised both as effector and detector.

In the case of the football World Cup, all the three mechanisms (security forces, emergency support and 'architecture') were utilised to a considerable extent, requiring however extensive intergovernmental co-ordination processes.[9] In the case of policing, the main 'safety' framework was co-ordinated through a 'Stab' (special unit) in the Federal Ministry of the Interior that however operated through the normal operating procedures of federal-Land (state) 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.

'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).

9

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

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 OSC, 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[10] are responsible for contingency and consequence management planning, such as the London mass fatality plan.[11]

The demands of a considerable security presence can strain the resources of Olympic organisers. At Athens 2004, heightened security concerns after the events of 9/11 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),[12] reflecting its reliance 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 of UK police manpower.

Organisation also refers to the set of 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 standardisation 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 standardisation of event schedules for sports events such as World Cups and Olympics, through guidance of international organisations 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 with 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 randomised 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-

[10] http://www.londonprepared.gov.uk/
[11] London Mass Fatality Plan, http://www.londonprepared.gov.uk/downloads/LMFPMainBodyV2.pdf
[12] London 2012 bid (2004). Chapter 12, p.39.

centred layout of the Olympic site presents a more complex challenge for mobilising 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.[13] 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 authorised vehicles. Security scanners at the entrance to public transport or competition venues provide off-site and on-site turnstiles for 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 effect and detect behaviour. In both cases under consideration, treasure was largely used to effect behaviour.

In the case of the football World Cup in Germany, 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* (the German army) was estimated to have been about €4.4m. 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

[13] Metropolitan Police Assistant Commissioner Tarique Ghaffur, quoted on BBC Online, 10 April 2008, 'Torch lessons for 2012 Olympic security'.

(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 organisers 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' (ARUP 2002a: 3-4), at a cost of £160.2 million (ARUP 2002b: 98). ARUP (2002b: 95) 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]'. 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 (House of Commons 2008: 9). Since then, security costs have been reported to reach £1.5 billion (Beard 2008).

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 30 years, and dramatically since Sydney 2000 – with the events of 9/11 (*Wall Street Journal*, 22 August 2004).

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 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 (Buck 2004). This rose to $415 million cover for Beijing 2008, at reported premium of $9.4 million (Lenckus 2008), 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 has been the added value of the tools of government perspective in understanding of security risk management at sporting mega-events? What do the observed patterns tell us about the politics of tool choice? And what value do these two questions have for wider interest in analysis of mega-events, and the FIFA Football World Cup and Olympic Games in particular?

Turning first to the question of the added value of the tools of government perspective, this analysis has demonstrated that the 'NATO' framework provides a systematic and insightful means for classification and comparison of the strategies employed by governments in securing mega-events. As an empirical analysis, this has moved towards a more institutional emphasis than Hood's original framework, but nevertheless the tools of government perspective provides an approach that highlights differences and similarities between cases that might otherwise be missed. Being forced to focus on four tools facilitates this systematic comparison. Using categories for the study of risk management in general not only provides for a more systematic comparison, but also for a more careful consideration of tool choice. For example, the emphasis on organisation in the two cases illustrates the complex and differentiated means through which governments seek to exercise visible control over security threats. Likewise, emphasis upon authority highlights the substantial differences in the resources available to the unitary UK state in contrast to its federal German counterpart. Thus, even with modification of the tools of government approach, there are analytical and empirical benefits of application of the 'NATO'-lens to categorise and compare the different approaches to security risk management.

In terms of tool choice, the paper introduced three well-known public policy explanations: *institutional isomorphism, functional response to differing risk profiles and responses defined by national political systems*. These alternative explanations of tool choice offer contrasting expectations as to what kind of patterns of tool choice might be expected for security risk management. As far as *institutional isomorphism* is concerned, there is limited evidence of cross-reading between the Olympics and the World Cup – in other words, there was limited evidence of the presence of causal mechanisms across the two mega-events associated with institutional isomorphism. Some replication of strategies was evident in terms of references to international security arrangements, but these tended to be generic. There does not appear to be an overarching sporting mega-event consultocracy that applies its recipes across events.

Such a finding is both surprising given the existence of national communities of (risk) practice. Perhaps linguistic and other barriers impede the transfer of experiences from one context to the other. The closed nature of national intelligence and security communities is another possible restraint to the isomorphism of security operations beyond the level of established international co-operation provisions (such as for policing).[14] While diffusion exists across football events and across Olympics, little

[14] Indeed, the closed nature of the intelligence world makes research into such networks of diffusion difficult, and might therefore lead to an under-reporting of isomorphic outcomes.

cross-reading takes place. Whether this is a result of the demands of different international bodies (IOC and FIFA) or of the perceived differences across the two events is difficult to tell, because when confronted with the similarities of the two mega-events (as illustrated above), actors clearly regarded them as comparable. Similarly, time does not seem to matter. Of course, critical junctures such as 9/11 or terror incidents during Olympics matter and provide for lessons, but they do not seem to provide for a basis that connects the demands on tool choice across mega-events. There is no unifying logic of tool choice that links together the events of Munich 1972 and Atlanta 1996 with planning for London 2012. The 7th July 2005 bombings, a day after the award of the Games, and British counter-terrorism policy in general, are a far more important reference point for local security than strategies put in place at Beijing 2008 or Vancouver 2010.

Instead, the evidence suggests that tools for security risk management in these cases evolve specific to the requirements of the specific sporting mega-event. This seems to reflect the distinct risk profile of each of the events – with differences in the use of organisation in particular reflecting the distinction between centralised and decentralised securing of the mega-event. Banning orders restricting the travel of football hooligans is not a relevant or appropriate tool in securing the Olympics – although there are similar requirements of border control and monitoring. The institutional framework of security also does not quite reflect differences in risk profiles.

The observed differences are not just function responses to the logic of the different risk profiles of these events, but also relate to the importance of national political systems in shaping tool choice. This is not altogether surprising. Political institutions allocate resources and therefore bestow legal and financial power to particular tools of risk management. Institutional jurisdictions also determine who is responsible for management of particular security risks – with consequences for the blame avoiding strategies of policy-makers and bureaucrats (Hood 2002: 15-37). At the same time, this also highlights a more general conclusion – that the political dimension of tool choice applies not just in terms of consequences of when things go wrong, but also in the close connection between aspirations to securitise mega-events and the world of high politics. The aim of government, in its regulatory form, is to eradicate risk and maximise social control. This suggests that despite the analytical value of generic classifications and theories of tool choice, empirical analysis of tools will never be able to detach itself from a close understanding of the political institutional context in which tool choice is conducted.

What does this discussion contribute to the wider study of mega-events and the Olympic Games and World Cups? For one, much of the discussion regarding these types of events has focused upon their symbolic, urban and cultural aspects and subsequent difficulties of how to manage such projects. Most football World Cups are remembered for the quality of football and the ultimate winner. The Olympics Games tend to be associated with headline-generating incidents and the visitor (and media) experience of the host city as well as with athletes' achievements on the track and

field. Such interests are perfectly legitimate. This paper has, in contrast, sought to advance understanding of risk governance of the World Cup, Olympics and mega-events in two respects. The first is to encourage – at a practical level – comparison between mega-events through the lens of tools that allow for systematic and detailed comparison of organisation. The limited extent to which the football World Cup and Olympics transferred strategies between one another is interesting both as a finding but also when considering the extent to which these mega-events share particular risk properties. On a conceptual level, this paper's integration of literatures on the tools of government and risk management at mega-events advances the discussion through enabling direct and clear comparison when most empirical analyses take the form of single-case studies. This promotes not just an analytical discussion of the tools and instruments of government in a fragmented domain, but also offers a new approach to analysis of strategies of risk management in a less understood terrain.

References

ARUP (2002a). *London Olympics 2012: costs and benefits. Executive summary* (21 May 2002). London: ARUP/Insignia Richard Ellis.

ARUP (2002b). *London Olympics 2012: costs and benefits* (Department of Culture, Media and Sport, Freedom of Information Request). London: ARUP/Insignia Richard Ellis.

Altshuler, Alan A. & Luberoff, David (2003) *Mega-projects: the changing politics of urban public investment.* Washington, DC: Brookings Institution.

Beard, Matthew (2008) 'Security costs will send 2012 bill over £10bn', *Evening Standard*, 29 September.

Boin, A. & 't Hart, P. (2003) 'Public leadership in times of crisis: mission impossible?' *Public Administration Review* 63 (5): 544-53.

Boin, A., 't Hart, P., Stern, E. & Sundelius, B. (2005) *The politics of crisis management.* Cambridge: Cambridge University Press.

Boin, A., McConnell, A., & 't Hart, P (2008) *Governing after crisis*. Cambridge: Cambridge University Press.

Buck, Graham (2004) 'Vaulting Olympic risk'. *Risk & Insurance* (August). < http://findarticles.com/p/articles/mi_m0BJK/is_9_15/ai_n6156490 >

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.

Flyvbjerg, B., Bruzelius, N., & Rothengatter, W. (2003) *Megaprojects and risk: an anatomy of ambition.* Cambridge: Cambridge University Press.

Flyvbjerg, B., Holm, M.S., & Buhl, S.B. (2002) 'Underestimating costs in public works projects: error or lie?' *Journal of the American Planning Association* 68 (3): 279-95.

Hall, Colin M. (1989) 'The definition and analysis of hallmark tourist events'. *GeoJournal* 19 (3): 263-68.

Hall, P.A. (1986) *Governing the economy*. Oxford: Blackwells.

Hall, P.A. and Soskice, D. (2001) 'Introduction to varieties of capitalism,' in P.A. Hall and D. Soskice (eds.), *Varieties of capitalism*. Oxford: Oxford University Press.

Hargrove, E.C. & Glidewell, J.C. (1990) *Impossible jobs in public management.* Lawrence, KS: Kansas University Press.

Hood, C. (1983) *The tools of government*. London: Macmillan.

Hood, C. (2002) 'The risk game and the blame game'. *Government & Opposition* 32 (1): 15-37.

Hood, C. (2007) 'Intellectual obsolescence and intellectual makeovers: reflections on the tools of government after two decades'. *Governance* 20 (1): 127-144.

Hood, C. & Margetts, H (2007) *The tools of government in the digital age*. London: Palgrave Macmillan.

Hood, C., Baldwin, R. & Rothstein, H. (2001) *The government of risk.* Oxford: Oxford University Press.

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.

Jennings, W. and Lodge, M. (forthcoming) 'London 2012: the politics of critical infrastructures and organising resilience' in B.M. Hutter (ed.), *Anticipating risks and organizing risk regulation*. Cambridge: Cambridge University Press.

Jones, B.D. & Baumgartner, F.R. (2005) *The politics of attention: how government prioritizes problems.* Chicago: University of Chicago Press.

Lascoumes, P. & Le Gales, P. (2007) 'Introduction: understanding public policy through its instruments – from the nature of instruments to the sociology of public policy instrumentation'. *Governance* 20 (1): 1-21.

Lenckus, D. (2008) 'Beijing 2008 Olympics cancellation cover led in Europe'. *Business Insurance*, 28 July.

Levy, B. and Spiller, P. (1994) 'The institutional foundations of regulatory commitment'. *Journal of Law, Economics and Organisation* 10: 201-46.

Linder, S.H. & Peters, B.G. (1989) 'Instruments of government: perceptions and contexts'. *Journal of Public Policy* 9 (1): 35-58.

Lijphart, A. (1999) *Patterns of democracies*. New Haven, CT: Yale University Press.

Lodge, M. (2007) 'Comparative public policy' in F. Fischer, G. Miller and M. Sidney (eds.), *Handbook of public policy analysis: theory, politics and methods*. Boca Raton, FL: CRC Press.

London 2012 bid. (2004) *Candidate file*. http://www.london2012.com/en/news/publications/Candidatefile/

UK Parliament. (2006). *London Olympic Games and Paralympic Games Act 2006 c.12*. < http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060012_en.pdf >

March, J.G. & Olsen, J.P. (1989) *Rediscovering institutions*. New York: Free Press.

March, J.G. & Olsen, J.P. (2009) *The logic of appropriateness*. ARENA Working Paper, 04/09. Oslo: Centre for European Studies, University of Oslo. < http://www.arena.uio.no/publications/wp04_9.pdf >Accessed 16 September 2009.

Moran, M. (2001) 'Not steering but drowning: policy catastrophes and the regulatory state', *Political Quarterly* 72 (October): 414-27.

Perrow, C. (1999) *Normal accidents: living with high-risk technologies*. Princeton: Princeton University Press. 2nd edn.

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.

Richardson, J. (ed.) (1982) *Policy styles in Western Europe*. London: Allen Unwin.

Roche, M. (1994) 'Mega-events and urban policy', *Annals of Tourism Research* 21 (1): 1-19.

Rosenthal, U., Charles, M.T. & 't Hart, Paul (eds.) (1989) *Coping with crises: the management of disasters, riots and terrorism*. Springfield, IL: Charles C. Thomas.

Salomon, L. (2002) *The tools of government: a guide to the new governance.* Oxford: Oxford University Press.

Simon, H. (1957) *Models of man: social and rational*. New York: John Wiley and Sons.

Wall Street Journal, 22 August 2004.

Websites

BBC Online Metropolitan (2008) 'Torch lessons for 2012 Olympic security', 10 April. < http://news.bbc.co.uk/1/hi/business/7340174.stm >

Germany. Federal Ministry of the Interior <http://www.bmi.bund.de/cae/servlet/contentblob/139756/publicationFile/15274/WM2006_Abschlussbericht_der_Bundesregierung.pdf >

London Resilience < http://www.londonprepared.gov.uk/

London Mass Fatality Plan
< http://www.londonprepared.gov.uk/downloads/LMFPMainBodyV2.pdf >