# Governing Mega-Events: Tools of Security Risk Management for the FIFA 2006 World Cup in Germany and London 2012 Olympic Games

Forthcoming in *Government and Opposition*.

Will Jennings, University of Manchester

Martin Lodge, London School of Economics and Political Science

**Abstract**

Mega-events represent a special venue for the practice of risk management. This paper analyses the 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. To what extent do strategies and practices of risk management resemble each other across events? And what explains similarities or differences in the tools of risk management observed in each of these cases? First, this paper explores three theoretical explanations of choice of particular policy tools or instruments. Second, it introduces the tools of government approach (Hood 1983) as a means to conduct direct comparative analysis of risk management across political and organisational settings and over time. The tools used for security risk management at the two mega-events are then compared and the different logics of tool choice are evaluated. This analytical approach offers a basis for future comparative enquiry into tools of risk management used in public and private organisations. The empirical findings highlight the particular importance of national political systems in influencing tool choice.

**Introduction**

Moments of crisis and the handling of post-crisis situations have attracted considerable 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.[1] Mega-events represent an important case for analysis of the management of security risks. These can be 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."[2] They combine both vast scale and scope with substantial interdependencies, resource commitments and geopolitical significance under the watchful eye of the international media and public. Less is known, however, about the degree to which strategies and practices of risk management resemble or draw on each other across mega-events and different organisational and political settings.

In parallel, public policy studies have seen a return to analysis of policy instruments and tools. This follows an earlier period in the 1980s when theoretical frameworks and typologies were applied to understand the means through which governments sought to affect and govern their populations.[3] The current revival revisits these approaches, and considers the extent to which trends over the two decades have impacted upon the nature of the tools of government in cross-sectoral and cross-national perspective.[4] Less is known about the tools of risk and crisis management, what logics underlie tool choice and the extent to which tool choice is shaped by distinct organisational and political settings.

This paper seeks to integrate insights from these two literatures. Most analyses of risk management trace decision-making processes, highlight organisational and operational failures, or advocate certain risk management strategies. This paper instead attempts to explore the logic of choice of risk management tools at mega-events. To do this, it analyses tools of security risk management for two sports-related mega-events: the FIFA 2006 Football World Cup in Germany and the London 2012 Olympic Games.[5]

---

[1] See C. Hood, R. Baldwin and H. Rothstein (2001). The Government of Risk. Oxford: Oxford University Press;  M. Power,  (2007). Organized Uncertainty: Organizing a World of Risk Management. Oxford: Oxford University Press; 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; A. Boin, A. McConnell, and P. t'Hart (2008) Governing After Crisis, Cambridge, Cambridge University Press; A. Boin, P. t'Hart, E. Stern and B. Sundelius (2005) The Politics of Crisis Management, Cambridge, Cambridge University Press.

[2] M. Roche (1994) 'Mega-Events and Urban Policy', Annals of Tourism Research 21(1): 1-19, p.1.

[3] S. Linder and B.G Peters (1989). 'Instruments of Government: perceptions and contexts', Journal of Public Policy 9(1): 35-58.

[4] L. Salomon (2002) The Tools of Government: A Guide to the New Governance. Oxford: Oxford University Press; P. Lascoumes and P. Le Gales. (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. A. Jordan; R.K.W. Wurzel and A.R. Zito. (2005) 'The rise of 'new' policy instruments in comparative perspective: has governance eclipsed government?' Political Studies 53(3): 477-496.

[5] C. Hall (1989). 'The Definition and Analysis of Hallmark Tourist Events', GeoJournal 19(3): 263-268. A. Altshuler and D. Luberoff. (2003). Mega-projects: The changing politics of urban public

This paper is organised as follows. First it formulates three hypotheses based on the theory of institutional isomorphism as to why some risk management tools are chosen rather than others and why, therefore, tools are chosen that resemble other tools in use in the same policy environment. It suggests that analysis needs to focus on competing templates in the context of decision-making following the logic of appropriateness. In other words it explores patterns of organisational (and therefore tool choice) homogenisation and differentiation.[6] Because policy domains are surrounded by multiple and fragmented policy environments, decision-makers face choices between competing sources for legitimisation and institutionalisation. We explore three distinct environments that offer templates for choice and legitimisation: the global environment of sporting mega-events ($H_1$), the idea of an event-specific environment ($H_2$), and the view that templates are drawn from distinct national politico-institutional constellations ($H_3$). Second it introduces the policy tools approach to analysis of security risk management, borrowing from Christopher Hood's 'NATO' (Nodality, Authority, Treasure and Organisation) approach. Third, it applies this toolbox framework to the case of security policies and organising templates for the FIFA 2006 Football World Cup in Germany and the London 2012 Olympic Games. This pair of cases maximises the leverage for possible analytical insight: Germany and the UK are developed and liberal-democratic European countries that are characterised by differences in political institutional framework. The focus of this analysis is the form and choice of the tools of risk management rather than the success or failure of these organising strategies, it therefore is not problematic that one event has taken place and the other is scheduled to take place two years from the time of writing (2010). As such, the case selection provides for an additional logic: if we want to discover to what extent the organising experience of a past event can influence decisions taken for an event scheduled to take place in the future, then it is essential to also focus on the time interval between the two events. In other words, explanation of what accounts for tool choice also allows us to recognise whether sporting mega-events are characterised by a common organisational field (by close ties to a common policy environment), or whether they are separated due to inherent differences between the events or the particularities of national political institutions. The paper concludes with an assessment of the relative power of the three explanations in light of observed patterns of tool choice and considers wider implications for analysis of policy tools and for the management of security risks in particular.

**Choosing Tools for the Job**

---

investment. Washington, DC: Brookings Institution; B. Flyvbjerg, N. Bruzelius, and W. Rothengatter. (2003). Megaprojects and Risk: An Anatomy of Ambition. Cambridge: Cambridge University Press; B. Flyvbjerg, M. Skamris Holm, and S. Buhl. (2002). 'Underestimating Costs in Public Works Projects: Error or Lie?' Journal of the American Planning Association 68 (3): 279-295.
[6] See P. DiMaggio and W. Powell (1991) 'The Iron Cage Revisited' in P. DiMaggio and W. Powell (eds) The New Institutionalism in Organisational Analysis, Chicago: Chicago University Press, p. 66. L. Jensen (2003) 'Policy Diffusion through Institutional Legitimation' Journal of Public Administration Theory and Research, 13: 521-41. T. D'Aunno, R. Sutton and R. Price (1991) 'Isomorphism and External Support in Conflicting Institutional Environments' Academy of Management Journal, 34: 636-61., P. Frumkin and J. Galaskiewicz (2004) 'Institutional Isomorphism and Public Sector Organisation' Journal of Public Administration Research and Theory, 14: 283-307. M. Lodge (2002) On Different Tracks, Westport, Praeger. M. Lodge and K. Wegrich (2005) 'Control over Government' Policy Studies Journal, 33(2): 213-33

What might make tools of risk management similar across different political and organisational contexts? The theory of institutional isomorphism suggests that a constraining process leads to homogenisation of organisational forms and practices 'that forces one unit in a population to resemble other units that face the same set of environmental conditions'.[7] Tool choice, as noted above, is dominated by the search for legitimate and apparently successful templates, and therefore by the logic of appropriateness. The influence of institutionalisation on organisational forms is now widely accepted, and focus has turned to the fragmented environments[8] that offer often competing templates and sources of legitimisation. In the context of tool choice, this paper is interested in two particular questions. First, what environments do the tools of security risk management for sporting mega-events draw upon? Second, what mechanisms shape the diffusion of particular tool choices?

This paper considers three organisational environments that represent distinct sources for tool choice: shared characteristics of sporting mega-events that encourage cross-diffusion across events such as football World Cups and Olympic Games ($H_1$), functional differences in the risk profile of World Cups and Olympics that leads them to inhabit separate organisational fields with, at best, weak linkages ($H_2$) and, finally, tool adoption that draws upon organisational templates dominant within the national politico-institutional system ($H_3$). The remainder of this section explores presence of these three environments in the context of mechanisms of institutional isomorphism.[9] Three mechanisms shape how competition between different sources of legitimisation (and therefore tool choice) is transacted. These are coercive (political, legal and other forms of resource dependency that induce homogenisation), mimetic (the imitation of best practice under conditions of uncertainty) and normative (the existence of consensus or a dominant professional set of doctrines) processes. Security risk management at sporting mega-events is linked to different environments through these mechanisms, enabling diffusion of the logic and practice of some tools of security risk management instead of others.

This section introduces these three hypotheses of tool choice and discusses the potential implications of tool choice for comparison of mega-events. The rest of this paper then considers to what extent these logics can persuasively account for observed patterns in the case of two sporting mega-events.

<u>$H_1$: Tool Choice Shaped by a Global Sporting Mega-Event Environment</u>

Sporting mega-events inhabit related fields, as events that share a number of common organisational characteristics related to their scale and scope, infrastructure and facilities requirements, resource commitments and geopolitical significance,[10] not to mention overlapping identities in terms of advertising and global TV coverage. At the heart of institutional isomorphism is assumption of linkages between and within organisational fields and also the extent to which uncertainty characterises decision-making. Related to this, coping with uncertainty is at the heart of decision-making when it comes to mega-events in general, and sporting mega-events in particular, for a

---

[7] DiMaggio and Powell (1991), p. 66.
[8] D'Aunno, Sutton and Price (1991).
[9] DiMaggio & Powell (1991), p. 67-74. Guler, Guillen & Muir Macpherson 2002, pp. 211-8.
[10] Roche (1994), p.1.

variety of reasons. Firstly, planning and operational decisions for mega-events are taken under conditions of high ambiguity and politicisation.[11] Sporting mega-events are similar in their exposure to optimism bias during the award and planning stages[12] and to risk aversion in the later operational stages,[13] each of which encourage tool selection in favour of pre-existing norms, protocols and standards (i.e. mimetic sources of isomorphism). Both mega-events are also exposed to similar security threats: they create a platform for protests or attacks where groups or individuals (e.g. anarchists, anti-globalisation protesters, terrorists) advertise their intentions to interrupt staging of the event. All these factors point to the inherent uncertainty that encourage searches for organisational strategies that are perceived to be legitimate or that have proven successful at previous events. Because conditions of risk and uncertainty are shared between World Cups and Olympic Games as a general organisational field it might therefore be expected that security risk management tools would tend to resemble one another across events and over time.

Secondly, the task of governing mega-events entails multiple uncertainties concerning prioritisation of risks, selection of indicators to monitor and evaluate information about risk, and use of policies or organisational instruments to mitigate threats or hazards and modify behaviour.[14] Risk management in all its forms is required to balance different priorities, but mega-events represent a special test due to their exceptional scale and complex design. Furthermore, the rotation of event locations restricts the pool of existing knowledge and experience to a small community of experts. In line with the argument stressing normative sources of isomorphism, the rise of a risk management consultocracy since the 1980s[15] might therefore be expected to contribute to the transfer of risk management knowledge and tools across international boundaries and across sporting events. Institutional isomorphism in the governance of risk at sporting mega-events would accordingly be manifested in the presence of dominant professional (or normative) logics of appropriateness in the choice of risk management tools that recur across different sporting mega-events.[16]

Finally, it is also possible to identify sources of coercive isomorphism, 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 problem of English hooliganism). Since the 1990s the International Olympic Committee (IOC) has specified standards for bid documents and conducted regular progress monitoring of Games organisation through its Evaluation and Coordination Commissions.

In sum, if the global environment of sporting mega-events affects tool choice (H$_1$) we would expect there to be similarities in the tools of risk management across mega-events. In addition, there would be some evidence of formal or informal

---

[11] M. Moran (2001). 'Not Steering but Drowning: Policy Catastrophes and the Regulatory State', The Political Quarterly, 72 (October): 414-427.
[12] RW. Pound (2004) Inside the Olympics. Toronto: John Wiley & Sons.
[13] Author.
[14] This is subject to cognitive and institutional biases ('friction') of attention identified in the model of disproportionate information processing, see B. Jones and F. Baumgartner (2005). The Politics of Attention: How Government Prioritizes Problems. Chicago: University of Chicago Press.
[15] M. Power (2007). Organized Uncertainty, Oxford, Oxford University Press.
[16] J.G. March and J.P. Olsen (1989) Rediscovering Institutions, New York, Free Press.

diffusion of knowledge and practice between events through coercive, mimetic or normative channels.

<u>H$_2$: Tool Choice Shaped by Event-Specific Environment</u>

Whereas the general field of sporting mega-events is suggestive of replication of tools of security risk management both across events and over time, variation in the risk profile of specific mega-events might instead be expected to be associated with separate organisational environments. In other words, the diagnosis of distinctive requirements of organising and securing the Olympics compared to the football World Cup can inhibit meaningful exchange in terms of drawing on security risk management tools across events. Instead the structural organisation of risk management knowledge around the distinct sporting mega-events (and their justification through reference to existence of a distinct risk profile) leads to differences in tool choice as tools are drawn from distinct environments (H$_2$).

It is not difficult to point to differences in securing the two sporting mega-events under discussion here that should facilitate selective rather than cross-cutting isomorphism to occur[17]: International football tournaments are associated with problems of public disorder, violence and organised hooliganism, with large crowds of supporters congregating in or around urban centres for specific matches. This contrasts with the Olympic Games and their 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 Olympic Games and international football tournaments are potential platforms for political demonstrations or terrorist attacks such threats are (historically) more prominent in the case of the Olympics, with historical precedents such as the riots prior to Mexico City 1968, the 1972 Munich Massacre, and bombing of Centennial Park in Atlanta in 1996. There are no similar security incidents in the context of football tournaments. The IRA bombing of Manchester city centre during the 1996 European Football Championships in England was not associated with the event and did not interrupt the competition.

Risk profiles also vary regarding geography and location. International football tournaments tend to be decentralised across 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 same time, this increases the demands on transport infrastructures to allow for the movement of large, often unpredictable number of fans (both directly to stadia and to public viewing areas). 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 determinant of whether security incidents prove critical, potentially forcing the interruption or abandonment of the event. In addition, this concentration of events on one central venue makes the the symbolic and reputational effects of breakdowns in Olympic security all the more powerful.

---

[17] This paper's research is based on extensive documentary analysis as well as interviews with key actors involved in security risk management at the FIFA 2006 World Cup in Germany and the London 2012 Olympic Games.

Significant differences also relate to the organizational scale and complexity. The London 2012 Olympics will host a total of 26 sports at 31 competition venues over 17 days of competition, bringing together an estimated 204 participating states, 10,500 athletes, 6,000 coaches and officials, 20,000 media, with around 500,000 visitors a day to the competition venues. The Games are to be policed by 15,000 police officers,[18] along with 6,500 private security contractors (according to provisional estimates).[19] This security task is of a different order from 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).

Overall, security risks associated with the Olympics tend to relate to geopolitical tensions and domestic or international terrorism. For football World Cups, large crowds of national supporters create security risks that are manifested in public disorder or violence and based upon longstanding territorial-cultural rivalries and tensions. As a result, tool choice should be expected for reflect the following patterns: While management of security risks for the Olympic Games tends to concern protection of critical infrastructures and trans-national coordination of intelligence services, for football World Cups security risks focus on maintenance of public order and effective crowd management, often with a distinct national flavour to policing styles (including exchange of some intelligence between national agencies and support from specialist units). The Olympics therefore involve surveillance of a different kind to that for international football tournaments (attempting to anticipate, detect and avert prospective attacks), whereas the latter are predominantly managed as a public order concern reliant upon street-level policing supported by cooperation between national police forces.[20] This difference in 'risk profile' diagnosis leads to the expectation that differences in risk management tools should be expected.

Processes of institutional isomorphism that draw selectively from the policy environment of 'Olympics' or 'World Cups' are therefore not unlikely. All three mechanisms, noted above, that link the event-specific policy environment to the choice of security risk management tools can be identified for particular mega-events. Coercive mechanisms exist given the institutional jurisdiction and regulations of international sporting authorities, mimetic mechanisms encourage the exchange of expertise within the domain of individual sporting mega-events (i.e. Olympic Games tend to draw on practice from past Games) and normative mechanisms contribute to the transfer of tools of security risk management by event-specific experts or consultants that share common professional norms and practices. While this has much in common with the first hypothesis, the perceived significance of distinctive functional requirements of sporting mega-events restrict formation of a common organisational field that could offer common tools as legitimate templates for organisation.

H₃: Tool Choice Shaped by National Political Systems

---

[18] Mayor of London (2004). London Assembly Questions on London bid for 2012 Olympic Games and Paralympic Games – 13.10.04. Answers to non-oral questions, prepared by London 2012, GLA, LDA, TfL 18.10.04, Q. 357/2004.
[19] London 2012 bid (2004). Candidate File, Volume 3, p. 39
[20] Of course, football world cups are also potential targets for threats associated here with those of the Olympics. We are making a point regarding emphasis.

The third organisational environment that is expected to shape tool choice refers to the effect of institutions on approaches to the management of security risks.[21] Political institutions and institutional design and jurisdictions shape the discretion of governments to select particular policies or tools;[22] as do policy styles and state traditions.[23] Institutional frameworks are expected to lead to differences in tool choice (H3), whether due to, for example, 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). Of the alternative mechanisms of isomorphism, <u>coercive</u> pressures emerge because of the existence of standard operating procedures within national systems of executive politics and government into which sporting mega-events are embedded, whether in terms of security policies and arrangements, constitutional rules shaping the allocation of institutional accountability and responsibilities or budgeting rules. With regard to <u>normative</u> pressures, national systems further shape rules of participation in decision-making. In other words, professional status and access can be influential in adoption of one type of policy tools rather than others.[24] In terms of <u>mimetic</u> pressures, particular national styles matter in terms of tool choice (for example, through the development of distinct professional cultures at the national level).

For this analysis, considerable differences in the choice of tools of security risk management might be expected given the differences between the German and UK political systems. Differences apply both to distinction between consensus versus Westminster democracies,[25] and between 'varieties of capitalism'.[26] Germany is governed through a system of executive and co-operative federalism (a 'unitary federal state'), requiring, for example, co-ordination of state police services (<u>Landespolizei</u>). Likewise, the German 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 (and most of all 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 such as the Metropolitan Police), and national departments and agencies along with Olympic organisations and the wider Olympic movement.

For national political responses to affect tool choice (H3) variation in choice of the tools of risk management should reflect national differences in institutional rules, structures and preferences.

---

[21] S. Linder and B.G Peters (1989). 'Instruments of Government: perceptions and contexts', pp. 49-50; M. Howlett (1991). "Policy Instruments, Policy Styles, and Policy Implementations: National Approaches to Theories of Instrument Choice," <u>Policy Studies Journal</u> 19: 1-21. Also A. Schneider and H. Ingram 'Behavioural assumptions of policy tools' <u>Journal of Politics</u>, 52(2): 510-29.

[22] R.K. Weaver and B. Rockman. (1993). <u>Do Institutions Matter?: Government Capabilities in the United States and Abroad</u>. Washington D.C.: The Brookings Institution. B. Levy and P. Spiller (1994) 'The Institutional Foundations of Regulatory Commitment' <u>Journal of Law, Economics and Organization</u>, 10: 201-46.

[23] J. Richardson (1982/eds) <u>Policy Styles in Europe</u>, London, Allen Unwin; P. Hall (1986) <u>Governing the Economy</u>, Oxford, Blackwells.

[24] Author.

[25] A. Lijphardt (1999) <u>Patterns of Democracies</u>, New Haven, Yale University Press.

[26] P. Hall, and D. Soskice (2001) 'Introduction to Varieties of Capitalism' in P. Hall and D. Soskice (eds) <u>Varieties of Capitalism</u>, Oxford, Oxford University Press.

The theoretical formulation of these three models of tool choice ($H_1$, $H_2$ and $H_3$) should not be interpreted as meaning that a single organisational environment determines adoption of tools of security risk management at the expense of the others. These hypotheses are not considered mutually exclusive. Nor are these explanations of tool choice exhaustive in representing all potential configurations of environments that a given mega-event might face. Nevertheless, these three policy environments capture dominant strains of thought in the collective literature on mega-events, organisations and public policy. The central question for this paper concerns which environment is most influential in tool choice and what are the mechanisms through which adoption of tools of security risk management occurs. This argument is summarised in Table 1.

[Table 1 about here]

**Comparing Tools of Security Risk Management**

To compare organisational strategies and practises of risk management, this paper adopts the policy tools approach introduced by Christopher Hood.[27] His framework offers a lens for the categorisation and analysis of those tools through which government interfaces with society, rooted in a cybernetic understanding of this relationship between the state and its citizens. The government toolbox of nodality, authority, treasure, and organisation ('NATO') is outlined in Table 2.

[insert Table 2 about here]

This paper combines Hood's generic analytical framework with assessment of our three hypotheses of tool choice. The framework enables direct comparison across cases and makes it possible to draw general inferences. This has advantages over an analysis based upon a descriptive chronology of each case. At the same time, this paper does not attempt to evaluate particular tools or tool mixes on the basis of outcomes. It therefore contrasts with most studies of tool choice that are concerned either with effectiveness or efficiency questions or in issue of visibility and intrusiveness.[28] We first of all undertake comparison of the form of the tools of risk management and analysis of the logic of tool choice, since these logically precede the effects and outcomes of interest to other studies.[29] It therefore should be possible to observe which environment is most influential in tool choice ($H_1$, $H_2$ or $H_3$) and through which mechanism, with regard both to use of individual policy tools as well as to across the wider portfolio of tools at the disposal of decision-makers. In this section, each of the tools of security risk management is introduced in brief before evidence is compared of their use in the management of security risks at the FIFA

---

[27] C. Hood (1983) <u>The Tools of Government</u>. London: Macmillan. C. Hood and H. Margetts (2007) <u>The Tools of Government in the Digital Age</u>. London: Palgrave Macmillan. (For reasons of parsimony and space, we do not expand this analysis by separating detectors and effectors, as considered by Hood and Hood & Margetts.)

[28] E.g. M. Howlett and M. Ramesh. (1993) 'Patterns of Policy Instrument Choice: Policy Styles, Policy Learning and the Privatization Experience', <u>Review of Policy Research</u> 12(3): 3-24. Howlett, Michael (1991). "Policy Instruments, Policy Styles, and Policy Implementations: National Approaches to Theories of Instrument Choice," Policy Studies Journal 19, 1-21.

[29] B.G. Peters (2000) 'Policy Instruments and Public Management' <u>Journal of Public Administration Research and Theory</u>, 10(1): 35-47; M. Howlett (2008) 'Managing the "hollow state" <u>Canadian Public Administration</u>, 43(4): 412-31.

2006 Football World Cup in Germany and in preparations for the London 2012 Olympic Games.

This paper is interested in comparing the tools of security risk management that were utilised in 2006 with those that form the organising template for 2012. This paper does not seek to answer the question as to whether either mega-event was more successful than the other in managing security risks. Whether or not security incidents of varying degrees occur at any given event does not necessarily indicate flaws in tool choice; there is such a thing as bad luck, even in the world of security. By definition, risk refers to the probabilistic weighting of adverse outcomes whereas outcomes in themselves do not shed light on how risks are anticipated and controlled. In terms of outcomes, the FIFA 2006 football World Cup in Germany suffered crowd disturbances at just three matches (Poland-Germany, England-Sweden and England-Ecuador). This relative absence of incidents was repeated at the UEFA 2008 European Football Championships. The rest of this section is interested in how the four tools of risk management manifested themselves in the context of these two mega-events, rather than in explanation of this outcome. We now consider each of the four tools in turn, also discussing factors affecting selection of each of these tools for the FIFA 2006 World Cup in Germany and the London 2012 Olympic Games.

**Nodality**

The tool of nodality denotes the extent to which government is a central point of contact in networks of information. This describes its capacity to receive and send information as well as to use information to modify behaviour of individuals. In the world of security risk management, nodality refers to instruments that facilitate information exchange between police, intelligence services and armed forces concerning the whereabouts and intentions of high risk individuals or groups. It also refers to the collection and analysis of intelligence about threats, spectators and traffic flows and the design and control of networks in order to prevent bottlenecks, redirect traffic and to mobilise police, emergency or security services to respond to problems. Nodality can therefore be equated with counter-terrorism and 'intelligent policing'. At the same time, it relies upon technical devices such as centralised and interconnected databases to check ticketing and visitor identities, especially at points of entry into a country (e.g. border controls). This also includes dissemination of public information for visitors and citizens about security, encouraging alertness and reporting of suspect activity or incidents. For the mega-events considered here, the tool of nodality was most prominent in the detection of security threats, in particular due to wider information exchange across national and international police forces.

For the 2006 FIFA World Cup, Germany built upon bilateral agreements with thirty-six other countries. These mechanisms had been utilised in previous European tournaments as well as at the Athens 2004 Olympic Games. As such, its security risk management strategy utilised existing arrangements that focused on information exchanges regarding particular fan groups (i.e. hooligans). These structures had emerged during the 1990s given the increased use of national team matches as platform for hooligan-related violence (one previously associated with club level football). Particular concern related to information regarding English, German and Polish hooligans, consistent with the specific risk profile of European football tournaments ($H_2$). As the 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 locations in which the tournament was held – a similar device had not been considered for the UEFA 1988 European Championship in Germany and it required temporary acceptance of shared and delegated forms of legal authority among police forces.[30] This replication of strategies within the field of football crowd management and policing is clear evidence of well-established procedures that shape security risk management tools ($H_2$). Somewhat more embedded in the German context of traffic management policy, other nodality-related tools were used to manage road traffic flows (the SOCCER transport research project). 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).

Similarly, in the case of the Olympic Games, 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 geopolitical context (e.g. the Beijing 2008 Olympic Games involved less formal international co-operation on intelligence matters than the Athens 2004 Olympics). This tool reflects the necessity of securing the Olympics against transnational terror threats, justifying the response by event-specific security risks ($H_2$). For the London 2012 Olympic Games, domestic intelligence agencies (e.g. the Joint Intelligence Committee, MI5, MI6, GCHQ, Defence Intelligence Staff) intersect with a number of Olympic-specific coordinating organizations: 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. The overall structure of these intelligence arrangements are, however, also a function of the jurisdictions and powers of existing institutions ($H_3$), so the pattern of tool choice for London 2012 reflects the centralisation of power in government agencies (with the exception of the Metropolitan Police which is London-centric rather than a national agency) that interact with external organisations. While there is evidence of the transfer of knowledge and expertise between Olympic Games, with secondment of Metropolitan police officers to the Integrated Security Unit at the recent Vancouver 2010 Winter Olympics,[31] there has been no similar interaction of the Met on security planning for London 2012 with security professionals from football World Cups.[32] The tool of nodality indicates the limited diffusion of practice between organisational fields ($H_1$) and the greater dominance of specific functional requirements ($H_2$). Even intelligence initiatives such as the Olympic Intelligence Centre (OIC) established at each Games since Atlanta 1996 to assimilate information and risk assessments through cooperation and information-sharing protocols involving over a hundred countries and international organisations have focused on intelligence of *Olympic* interest. Nodality tools therefore tend to emerge within the context of specific Olympics or World Cup experiences which are then embedded within the context of national administrative arrangements.

**Authority**

---

[30] 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/).

[31] Interview, Official, Integrated Security Unit, Vancouver 2010 Winter Olympics.

[32] Interview, Official, Metropolitan Police.

Authority refers to the legal power of government and other sources of social or political legitimacy. This refers to tools that enable government, at all levels, to promote or compel behaviour, as well as to license and to prohibit activities. This includes legal controls on individual movement, power of prosecution and imprisonment, censorship and procedural devices to limit demonstrations, as well as authority to deal with ticket touts, criminal activities, prostitution, the licensing of drinking establishments, and measures that impede the movement of dangerous (i.e. high risk) groups or individuals such as hooligans, extremists or terrorist suspects. Overall, the tool of authority extends to authorization of planning permission and the 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).

Organising bodies for both Olympic Games and World Cups typically rely on private law companies or associations; e.g. the London Organizing Committee for the Olympic Games (LOCOG) and the German Football Association (DFB). These organisations operate with the support of public agencies (at various levels of government) for provision of infrastructure, security and other essential services.[33] Tools related to authority therefore draw heavily upon national political styles and institutions (H3). This also relates to government guarantees that are part of any World Cup bid. In the German case, the authority to manage security risks constitutionally resided with the Land (state) level. For the World Cup, security risk management was, as a result, managed through a wider (established) political-intergovernmental process in which the lead Land (North Rhine Westphalia) together with other Land governments, the Federal Ministry of the Interior, and the DFB developed the agenda. The most prominent aspect in which federal government utilised the tool of legal authority was through its reinstatement of border controls which allowed it to refuse entry to those individuals associated with security risks (i.e. hooligans). This reflected the crucial importance of interception of known troublemakers to the policing of international football tournaments (adding to the legitimacy of organising templates that refer specifically to international football tournaments). Public viewing events were steered through licensing and other security standards, along with local policing (i.e. organisation). Security was dominated by negotiated solutions within the intergovernmental process, as well as within the network of emergency responders, headed by a federal agency, the Technisches Hilfswerk (see below).[34] The German political system therefore equally shaped the deployment of tools of risk management (H3).

The legal framework for staging the London 2012 Olympic Games[35] presents a fragmented set of security jurisdictions and responsibilities across the Department for Culture, Media and Sport, the Home Office, the Olympic Delivery Authority (ODA), LOCOG and the Metropolitan Police (within the Home Office). This has shaped the security programme for London 2012, and thus the architecture of tool

---

[33] The use of legal authority to suspend work permits, working hours, or customs clearance regulations are not considered here.

[34] Apart from the federal complication, there was a further inherent tension 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 mainly concerned issues of sponsorship rather than security risk management measures.

[35] 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.

formation ($H_3$). Although the police, security and emergency services for the London 2012 Olympic Games operate within defined jurisdictions, they are co-ordinated through a single Olympic command structure:[36] Central government is responsible for securing the Olympics despite the lead role of LOCOG in staging the Games and the ODA in delivering the main venues. This is consistent with the classic Westminster model of British government, indicating the sustained influence of national governing styles ($H_3$). The ODA and LOCOG retain authority over integration of security in the 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, 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 that reflect national political institutions and their organisational tools ($H_3$).

These divisions in the distribution of authority introduce considerable tensions with regards to risk prioritisation; in particular between perceived priorities that were directly linked to event-specific risks ($H_2$) and institutional jurisdictions ($H_3$). It thus represents a potential source of ambiguity and tension over responsibilities for the management of security risks associated with infrastructure and operations. For example, the hardwiring of security into building design through reinforced concrete and barriers is coordinated by the ODA, while the Metropolitan Police and intelligence services are responsible for counter-terrorism strategy and operations. Overall, the tool of authority therefore tends to be correlated with the influence of national political institutions ($H_3$) in determining organisational jurisdictions and powers as well as the conduct of security operations on the ground.

## Treasure

Treasure denotes the access of government to assets and financial resources. For example, financial subsidies or taxes supposedly modify individual behaviour. In the context of security risk management, treasure refers to application of financial strength for direct expenditure on security or indirect provision of insurance and assurance services (with governments acting as lender of last resort). It also includes public spending on construction and operation of buildings, such as stadiums. Treasure is also required for payment of private suppliers/contractors: e.g. firms contracted to provide support for public security and defence services and funding of third-sector (charities) emergency services that are not direct part of the government apparatus, but exist somewhere in the twilight zone between public and private sectors. In both mega-events, treasure was largely used to finance security operations with the aim of reducing security risks.

In the case of the 2006 World Cup, it is difficult to calculate the exact amount of expenditure on security risk management because this was diffused both between

---

[36] See London 2012 bid (2004) Candidate File.
http://www.london2012.com/en/news/publications/Candidatefile/

levels of government and between private and public organisations (demonstrating the complexities of accounting for security that can result from sharing of responsibilities across political institutions, $H_3$). Federal investment in transport infrastructure was classed as independent of the World Cup (estimated to be €3.7bn). Financial support for modernisation of two stadiums (Berlin and Leipzig, nearly €250m) was provided (all stadiums were renovated or rebuilt, but not with federal financial support). The full economic cost for the use of the army, the <u>Bundeswehr</u>, was estimated to have been about €4.4m. Other measures such as use of the federal police were budgeted through normal budget lines, whereas the deployment of NATO reconnaissance flights was paid for through the NATO budget (as had been the case with the 2004 Olympics and European Championships). The overall structure of funding therefore was a product of the German political system ($H_3$). However, the federal government was not lender of last resort for the World Cup and the financial risk of staging the event instead resided with the German football association.[37]

For the London 2012 Olympics, treasure includes direct expenditure by both public bodies (e.g. the Home Office and Metropolitan Police) and expenditure by private or quasi-private organisations (e.g. LOCOG) on the public good of security. The overall security budget is the responsibility of central government, with the exception of the security arrangements for the main Olympic site in the Lea Valley. The latter, a fraction of the total, is funded through LOCOG's revenue from tickets, sponsorship and merchandise. The burgeoning budget for security for the London 2012 Olympic Games illustrates how forecasting and management of security costs is a significant concern for sporting mega-events, exhibiting a common feature of organisation in the Olympics domain in particular ($H_2$). Moreover, cross-referencing of security costs linked budget estimates to previous Olympic Games, rather than sporting mega-events in general. The initial feasibility study for a London bid to host the Olympic Games included in its balance sheet 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",[38] estimated at a cost of £160.2 million.[39] The consultants 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]".[40] Site security was costed at £190 million in the bid submitted to the IOC but increased to £268 million in the revised March 2007 budget which put the total security and policing cost at £600 million.[41] While comparison between different Olympic Games is difficult, the cost of security at the Olympics has grown over the past thirty years, and dramatically since Sydney 2000.[42] This demonstrates some of the security pressures that are acute for Olympic organisers in particular ($H_2$), but

[37] The World Cup generated a substantial surplus for the association (€135m, the DFB's net benefit was €56.6m). The bid to host the tournament likewise was funded through private finance. In contrast, the unsuccessful Berlin bid for the 2000 Olympic Games was estimated to have cost approximately €31m in public funds.

[38] ARUP (2002). <u>London Olympics 2012: Costs and Benefits, Executive Summary</u> (21 May 2002). London: ARUP/Insignia Richard Ellis, pp. 3-4

[39] ARUP (2002). <u>London Olympics 2012: Costs and Benefits</u> (Department of Culture, Media and Sport, Freedom of Information Request). London: ARUP/Insignia Richard Ellis, p. 98.

[40] Ibid, p. 95.

[41] House of Commons, Public Accounts Committee. (2008). <u>The Budget for the London 2012 Olympic and Paralympic Games. Fourteenth Report of Session 2007-08</u>. London: The Stationery Office Limited. p. 9.

[42] D. Roberts (2008). 'Olympics Security Is No Game,' <u>BusinessWeek</u> (7 August 2008).

nevertheless are of wider influence in organisation of sporting mega-events since the events first of the Munich Massacre in 1972 and later of September 11, 2001 ($H_1$).

Treasure also includes insurance to provide for a form of asset protection and remediation. Since the events of 9/11, insurance premiums for sporting mega-events have risen sharply as projected security risks have proliferated. The IOC purchased insurance cover ($170 million) for the first time for the Athens 2004 Olympic Games, to protect against financial losses of cancellation due to terrorism or natural disaster (at a reported premium of $6.8 million).[43] This rose to $415 million cover for Beijing 2008, at a reported premium of $9.4 million,[44] so might be expected to rise again for London 2012. As such, treasure mechanisms are used to protect against security risks that also pose treasure risks (in terms their consequences for the financial viability of the Games). Again, this reflects the dominance of the event-specific environment of the Olympics in shaping this policy ($H_2$).

## Organisation

Finally, organisation refers to capacity of government for undertaking direct action, for example in its mobilisation of bureaucrats or the armed forces. This refers to physical ability of government to intervene in the affairs of its citizens and other states or to otherwise to act as a deterrent. It extends to the design and configuration of event architecture in a broader sense and operation of technologies of social control such as CCTV. Organisation includes devices that reduce bottlenecks, such as in the case of transportation, or create them, such as in the management of visitor flows and the operation 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.

In the case of the 2006 Football World Cup, organisation related to the use of security forces, emergency support services and architecture. This involved extensive intergovernmental co-ordination (facilitated by the NICC),[45] especially with regard to policing (as noted earlier). The main 'safety' framework for policing was co-ordinated through a task force ('Stab') in the federal ministry of the interior, operating under thee normal procedures of federal-Land co-operation (the intergovernmental standing committee of interior ministers). A sub-committee dealt with policing and crime. Co-operation involved the engagement with other national police forces; with 570 foreign police active in Germany to monitor fans and to advise domestic security forces. This further demonstrates the influence of national political institutions on policing ($H_1$). In terms of non-policing security measures, the Länder were solely responsible for fire, rescue and emergency services. In contrast, however, the task of overall co-ordination was managed through two federal agencies: the Technisches Hilfswerk, which were largely in control of emergency services (especially in terms of infrastructure, e.g. communications, electricity) and the Bundesanstalt für Bevölkerungsschutz und Katastrophenhilfe, which provided additional equipment as well as training for local emergency services. The army was also utilised to provide medical services (as well

---

[43] G. Buck (2004). "Vaulting Olympic risk", Risk & Insurance (August, 2004).
[44] D. Lenckus (2008). 'Beijing 2008 Olympics cancellation cover led in Europe', Business Insurance (28 July 2008).
[45]

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

as offering a support policing role which was not called upon). Overall, then, despite pressures for cross-border isomorphism ($H_1$), organisation was dominantly shaped by the domestic institutions of German policing and security ($H_3$).

For the World Cup, the tool of organisation was not just a matter of personnel, but also was exercised through stadium architecture and 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 already in regular use for football matches, but that the staging of the Confederations Cup provided a dress rehearsal for insights into potential security risks (indeed, the equivalent dress-rehearsal revealed glaring failures in South Africa's preparations regarding stadium security arrangements). The issue of design of football stadiums pointed to the importance of the football-specific domain in the context of running the World Cup, given the presence of international guidelines in terms of architecture. In addition, the tools of tournament policing were shaped by the domestic institutions in the deployment and command of security-related personnel ($H_3$).

For London 2012, the network of organisations and manpower involved in the security operations for the Olympic Games involves high-level coordination through the Cabinet-level Olympic Security Committee and a range of government agencies that deal with particular security tasks: MI5, the UK's domestic counter-intelligence and security agency, and other intelligence services are responsible for gathering, disseminating and advising on intelligence matters, the Metropolitan Police and regional police forces provide policing, law enforcement and emergency responses and the London Resilience Team[46] are responsible for contingency and consequence management planning, such as the London Mass Fatality Plan.[47]

The demands of supplying a substantial security presence can place a strain on the resources of Olympic organisers. At the Athens 2004 Olympics, heightened terror alert levels after 9/11, informed the deployment of 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 from the European Union. The projected number of police for the London 2012 Olympics, at 14,800, is far lower (even when counting the additional support from 6,500 private security contractors),[48] reflecting its greater reliance upon intelligence-gathering and processing instead of policing. That number for London 2012 is not insignificant, however, since it represents about 10% of the total UK police resource. Although strongly influenced by pressures of isomorphism due to the common threats of international terrorism confronting mega-events, the structure of Olympic security organisation reflects pre-existing organisational jurisdictions and powers of domestic institutions - the choice of policy tools is therefore more a matter of domestic institutions ($H_3$) than drawing on global mega-sporting event templates, although the wider international security debate did of course inform debates about the types of security risks that organisers were to organise against.

The tool of organisation also refers to event features that, like transport hubs and infrastructure, determine the physical spacing, timing and structure of crowd flows and security provisions, as well as facilitating control and responsiveness in the

---

[46] http://www.londonprepared.gov.uk/
[47] London Mass Fatality Plan, http://www.londonprepared.gov.uk/downloads/LMFPMainBodyV2.pdf
[48] London 2012 bid (2012). Candidate File, Chapter 12, p.39.

case of incidents. For example, standardization in stadium designs and emphasis upon the importance of creating similar response environments reduces the problems associated with lack of familiarisation among first responders in emergency situations – which is one respect in which sporting mega-events transfer organisational practice and experience across events, pointing to the presence of considerable communication across sporting mega-events ($H_1$).

The Olympic Village (within the Olympic Park area) housing all athletes and support staff for London 2012 creates a general perimeter that requires securing. As most events are to take place in the Park – at the main stadium and aquatics centre – this leads to a high concentration of security efforts at a single site. In contrast to the enclosed architecture of football stadia, however, the main Olympic site that has been a common feature of most recent Games 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 randomised and 'intelligent' surveillance inside the site, with different levels of security within the Olympic Park. 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 main Olympic site presents a more complex challenge for mobilising intelligence and presence for the purposes of security. The functional characteristics of Olympic and football stadia therefore give rise to differences in the sorts of security operation encountered ($H_2$).

The key differences between the two mega-events are summarised in Table 3.

[insert Table 3 about here]

## Comparing Tools of Security Risk Management

The discussion has revealed a diverse set of security tools in the two cases. Each of the tools corresponds to a particular aspect of the security environment and the response of government and private organisations to threats or hazards. The tool of nodality, observed most often in the form of counter-intelligence activities, risk assessments and intelligence sharing or exchange, reflects the importance of information for decision-making both in strategic design of risk management systems and in organisational disruption or prevention of threats. The tool of treasure is symptomatic of the dependence upon financial resources to finance security operations, to fund secure infrastructure and stadium designs, and to purchase additional support (e.g. private security contractors) or insurance against security incidents. This highlights tension between public and private goods, when the security risks of such mega-events are assumed by the state, but commercial profits accrue to private bodies such as the IOC or FIFA and local Olympic organising committees and national football associations. Financing of security for mega events therefore is venue for political tension between public and private interests. The tool of organisation is most visible in policing operations at street-level, as well as in the physical architecture of event venues and infrastructure which determine the context of both security threats and responses. Such mobilization of police manpower is integral to the deterrence, detection and disruption of security threats. Finally, the tool of authority is pervasive in determining the legal authority and power of the state to

intervene, control and mobilize both its organisational forces and its citizens. For transnational mega-events such as the Olympics and football world cups, this is essential to effective operation of border and immigration controls, and to its exercise of social and technological controls – such as travel restrictions and wire-tapping of phones and internet communications of suspected terrorists. This tool also provides a basis for mobilization of different organisational resources of the state, such as the police and armed forces. In sum, the tools of government framework provides a systematic means for classification and comparison of the strategies employed by governments and private organisations in securing mega-events. It highlights differences and similarities between cases that might otherwise be missed – and indeed it points to the centrality of national governments in risk managing sporting mega-events regardless of the formal organisation 'at a distance' through national sports associations/Olympic committees. Finally, being forced to focus analysis on the four tools facilitates systematic comparison across cases and over time.

This analysis has demonstrated that, the security risk management of these two sporting mega-events reflects their particular location within a number of (fragmented) organisational environments. The differentiation between sporting mega-events, specific-mega-events and national politico-institutional system offers not just analytical insights as to why particular tools are more prominent in one case than the other, but also practical insights into the extent to which the two mega-events might draw on each other.

As far as a global environment of sporting mega-events is concerned ($H_1$), there is limited evidence of cross-reading of risk management tools between the Olympic Games and football World Cup. There are, in practice, largely two worlds of sporting mega-events with no clear causal mechanisms of diffusion or exchange across the two mega-events (consistent with the event-specific hypothesis, $H_2$ ). 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.

Within each of the sporting mega-events, there was considerable evidence of institutional isomorphism: especially in the form of the drawing on experiences from previous events as well as the utilisation of expertise from earlier events. For example, the German DFB was actively involved in advising South Africa on its security risk management preparations[49], and part of the convention for football mega-events is that organisers include representatives of the next host nation in their security planning: representatives of the 2008 Swiss/Austrian European Championship organisers were involved in the 2006 World Cup security committee. Olympic security advisors also move between Games. For example, the New South Wales Police Commissioner responsible for the Sydney 2000 Olympic Games, Peter Ryan, served as Principal Security Advisor to the Athens Olympic Games Organising Committee and is security expert for the IOC. In planning for London 2012, Metropolitan Police officers were seconded to the Integrated Security Unit responsible for security at the Vancouver 2010 Olympic Games. All three sources of institutional isomorphism were present in the cases: with some coercive measures in prescribed standards or procedures that required implementation, both informal and

---

[49] Interview, German football association.

formal mimicking of security provisions and templates, and professional/normative processes observed in the prevalence of risk consultants and in networks of experts. However, there was no evidence of a substantive cross-fertilisation between mega-events, despite the considerable similarity in some of the security risk management tools and threats.

Such a finding is surprising given the existence of international communities of (security risk) practice. Perhaps linguistic and other barriers impede the transfer of experiences from one context to the other, though this does not appear to be the case within-event for either the Olympics or the World Cup. 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).[50] Similarly, the relative lack of diffusion could be associated with the demands of different international bodies (IOC and FIFA) or because of the perceived differences across the two events is difficult to tell. When confronted with the similarities of the two mega-events (as illustrated above), interviewees 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 London bombings on 7 July 2005, 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.

In interviews, security officials from both Olympic and football worlds shared the view of distinct organisational fields that offered limited scope for cross-reading between events. When prompted, however, there was agreement that in the area of security risks in particular, there was potentially much similarity in risks and security vulnerabilities. Interviewees noted that apart from the different organisational challenges (e.g. decentralised vs. centralised staging of events) hooliganism was a primary risk for international football tournaments, while transnational terrorism was a principal concern for the Olympics. At the same time, interviewees questioned the continued prominence of this claim in light of recent changes in the global security environment. Tools for security risk management are therefore to some extent designed in response to specific requirements of the sporting mega-event. Differences in the use of organisation in particular reflected the distinction between centralised and decentralised securing of the mega-event. Banning orders (the use of authority and nodality) that restrict travel by football hooligans are not a relevant tool in securing the Olympics, though there are similar requirements of border control and monitoring for detection and interception of terrorist suspects. In general, however, the evidence suggests that differences in risk profile are not that decisive in choice of tools of risk management. Rather, as implied by the theory of institutional isomorphism, it is the perception of difference that matters - and here the linkages between the event-specific environment and the mega-event in question reinforced (through all three mechanisms) the drawing on tool templates from preceding events given the legitimatisation that Olympics and World Cups were distinct events.

---

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

Finally, to what extent can national institutions ($H_3$) explain differences between the 2006 World Cup and the 2012 Olympics? 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 substantial differences in the resources available to the unitary UK state in contrast to its federal German counterpart. Political institutions allocate resources and as such 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.[51] More generally, therefore, 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.

**Conclusion**

What does this discussion contribute to the wider study of mega-events and the Olympic Games and football World Cups? This paper has 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 analytical framework of tools of risk management that enables systematic and detailed evaluation of organisation. As an analytical method, the tools framework allows for direct comparison of approaches, both across domains and across time. The limited extent to which the football World Cup and the Olympics transferred strategies between one another is interesting as a finding especially when considering the extent to which these mega-events share particular risk properties – not least their exceptional scale. Despite the significant overlap in security risk profile, the evidence suggests that in terms of isomorphism there are two worlds of sporting mega-events in which Olympic Games tend to draw on each other while international football tournaments tend to draw on other football tournaments. On a conceptual level, integration of literatures on the tools of government and risk management at mega-events advances analysis through enabling direct and general comparison when most studies use single cases or domain-specific frameworks. This promotes not just analytical discussion of the tools and policy instruments of government in a fragmented domain, but also offers a new approach to the analysis of strategies of risk management in a less well understood terrain.

---

[51] C. Hood (2002) 'The Risk Game and the Blame Game'. Government & Opposition 32(1): 15-37.

**Table 1.** Overview of Logics of Tool Choice

| Policy Environment | Tool Choice | Mechanism |
|---|---|---|
| Global Sporting Mega-Event Environment | Tool choice draws on experience of sporting mega-events at large | Coercive: international conventions, guidebooks and commercial requirements<br>Mimetic: searching for legitimate templates across events<br>Normative: existence of security risk consultocracy universe |
| Event-Specific Environment | Tool choice draws on experience within domain | Coercive: existence of international conventions and organizers (IOC & FIFA)<br>Mimetic: organizers draw on templates experienced by predecessors<br>Normative: existence of a distinct World Cup and Olympics security risk management community |
| National Political System | Tool choice reflects dominant standard operating procedures of national political system | Coercive: presence of constitutional and budgetary rules shape tool choice<br>Mimetic: Central actors are selected by distinct national rule patterns therefore influencing professional background and participation<br>Normative: dominant professional worldviews |

**Table 2.** The Tools of Government (from Hood 1983, Hood and Margetts 2007)

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

**Table 3.** Differences in security risk management tools between 2012 and 2006

| Treasure | Nodality |
|---|---|
| Key difference in Olympics requiring the state to be lender of last resort and to support construction of the main Olympic site and facilities. | Key difference in perceived variation in security risk with football requiring specific focus on hooliganism and the monitoring of large crowds in and across specific locations. |
| **Organisation** | **Authority** |
| Similar organisational demands with differences reflecting national jurisdiction. Football allows for near-weekly rehearsals of security management (in most cases) given national football competitions. | Limited differences in need to license or restrict individual activities. Differences largely due to national jurisdictional allocation of legal competence. |