SUSTAINABILITY OF THE OLYMPIC GAMES: SECURITY ASPECT

Research Paper

Luka Lesko, College of Occupational Safety and Health; Swiss School of Business and Management, Geneva, Switzerland, luka@ssbm.ch

Mario Silic, College of Occupational Safety and Health; Swiss School of Business and Management, Geneva, Switzerland, mario@ssbm.ch

Gal Oberhofer Dimitrijevic, Swiss School of Business and Management, Geneva, Switzerland, gal@ssbm.ch

Abstract

The Olympic Games require one of the most complex mass event-related security operations in the world. Using both theoretical and empirical knowledge, this research on governance, work scope and budget for security and safety within the summer Olympic Games from Sydney 2000 to Tokyo 2021 (six case studies) provides a comparative analysis and future perspectives in the domain of Olympics-related security and safety. Terrorism remains the greatest threat to the Olympics due to the scale of direct and indirect effects while cyber-attacks are becoming an extremely threat. Although the security budget occupies a significant share of the total organizational budget of the Games, those investments can be justified by long-term legacy. Further research should address the methods to optimize security measures against restrictions of human rights and liberties, as well as on prevention of inter-agency rivalry and prevention of cyber-attacks at the Olympic Games.

Keywords: Major sporting events, terrorism, cyber, costs.

1 Introduction

Security studies are located between several disciplinary approaches, it is a type of knowledge that follows not only the logic of academic/scientific work but also the requirements of the national establishment and public expectations (Bilandžić, 2014). Both history and the recent period indicate an expansion of the scope of security. Security studies are a scientific field in evolutionary continuity. Security is not a fixed or dispositional, but a dynamic and complex process, never final and fully completed, security needs are constantly produced and reproduced (Bourbeau, 2015).

According to Buzan and Hansen (2009), security is more comprehensively understood by analyzing a number of related concepts: complementary concepts (strategy, deterrence, humanitarianism), parallel concepts (power, sovereignty, identity) and opposition concepts (peace, risk, state of emergency). It is also a framework for the systematic inclusion of sport, as a parallel concept, in explorations, explanations and interpretations of security (Bilandžić and Leško, 2019). Sporting events play a major role in constructing national identity, but they are also a means to achieve political goals (Coakley, 2009). Sport is suitable for political instrumentalization because sporting events take place constantly, within the country and internationally, and thus sport is used for political purposes more conveniently and more often than other social activities (Bilandžić and Leško, 2019). Both theoretical and empirical data prove it is justified to observe sport in a security and safety context. In the 20th and 21st centuries, terrorism affected various social phenomena, including sport as an integral factor of society. Giulianotti and Klauser (2012) tried to construct a specific theory that links terrorism and sport (sport/terrorism couplet). A key question is how the securitization can be balanced with democratic principles and respect for human rights and civil liberties (Spaaij, 2016). One of the goals, but also the means in achieving the main goal of terrorism, is the production of fear and social anxiety (Walsh, 2016). This also applies to societies that seem strong from the outside, but terrorism indicates their vulnerability. The most common targets of terrorist attacks in the world in general, which primarily include civilians and civilian institutions (Bilandžić, 2014), indicate a causal relationship that determines sports facilities as targets of terrorist attacks. Mass gatherings, pre-known dates of matches, high concentration of emotions, fun, carefreeness and achieving publicity without much expense make sports facilities attractive soft targets of terrorist attacks (Leško, 2018). The Olympic Games require one of the most complex mass event-related security operations in the world. The International Olympic Committee (IOC) assesses the capability of the country to provide appropriate security to safely host the Games so security is one of the crucial (and one of the most expensive) segments of staging the Olympic Games. The IOC stipulates that security issues are the sole responsibility of the host city because it is unwilling or, more accurately, unable to meet the demands it would face (Bellavita, 2007). According to the IOC (2015) ensuring the safe and peaceful celebration of the Olympic Games is the responsibility of the relevant authorities of the host country, through coordinated planning and organization with the host city's Organizing Committee for the Olympic Games. A multi-agency strategy should be adopted to involve all government ministries, law enforcement agencies and other stakeholders involved in the planning and delivery of security. These entities typically include the Organizing Committee, the home affairs ministry, the ministry of defense, intelligence agencies, cyber-security agencies, the police and immigration and/or customs agencies. According to the IOC Candidature Acceptance Working Group (2008) the following sub-criteria were taken into consideration: the incidence and likelihood of terrorism; the levels of known recorded crime and other public safety issues; the overall technical and professional competencies of the main security forces and the proposed command and control; the existing investment in security and related technology and the proposals to improve in this area to meet the Olympic Games security requirements; the complexity of the proposed Olympic Games “theatre of operations” and the required security response. The Olympic Games in the post 9/11 era of terrorism represent opportunity, a significant example of what Toohey and Taylor (2007) term “terrorist capital”. The global stage that the sport mega-event provides arguably makes the Olympics attractive to terrorists who seek to inflict maximum damage and fear or to maximize publicity for their campaigns (Spaaij, 2016). This is exacerbated by the reality that it is a live event televised around the globe to billions of people (Noble,

2007). Proven empirical data confirms that claim. As a result of such incidents, security and counter-terrorism strategies have been implemented as core concepts in the organization of mega sport events (Giulianotti and Klauser, 2012). Fears resulted in the International Olympic Committee becoming increasingly anxious about security and the requirement for Olympic hosts to compile sophisticated security packages in cooperation with national and international authorities. This development and the resulting financial gigantism of the Olympic Games has led local residents to reject the possibility of hosting the event, as has been witnessed on a regular basis in current bidding processes for Olympic Games (Krieger, 2019). Despite that, terrorism and security have received less academic scrutiny than other aspects of the Games (Spaaij, 2016). Security, including counter-terrorism strategies, has become one of the most important parts of the preparation of major sporting events (Savitch, 2003), leading to a multiplication of security budgets (Giulianotti and Klauser, 2012). Although security investments are not sustainable and not produce future economic revenues. However, they are indispensable to stage mega sport events in the present day and constitute a key concern for a sport organization such as the IOC already during the bidding process (Houlihan and Giulianotti, 2012). Bidding cities must calculate security costs in their original financial plans, leading to high projected costs for all stakeholders. The cost eruptions as a result of safety operations have led to new "fears" on staging the Olympic Games. In the last years, the majority of the population in potential host cities has rejected, when asked, the organization of the Olympic Games (Krieger, 2019). In the other hand, it is broadly agreed that Olympic security arrangements can endure long after the event is over. Post-event security legacies are now a strategic issue in Olympic security planning (Bennett and Haggerty, 2011). Security legacy has evolved into an explicitly articulated component of the Olympic business plan intended from the outset to capitalize on an opportune moment in order to accelerate the expansion of security capabilities and surveillance infrastructures (Boyle, 2012). In addition to technological, informational and knowledge legacies, they include the endurance of attitudes about security and surveillance whereby the Olympic "state of exception" can become normalized (Bennett and Haggerty, 2011). Moreover, the Olympic Games serve as an opportunity for the authorities to introduce security measures that would be more difficult to justify in normal circumstances (Bennett and Haggerty, 2011).

The lack of comparative research on the sustainability related Olympic security and safety as one of the most demanding and expensive segments of project management of such events, led to the creation of research objectives.

2 Methodology

This research has three main objectives and one sub-objective:

1) Main objective 1: Comparative analysis of security and safety governance of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016 and Tokyo 2021 Olympic Games.

2) Main objective 2: Comparative analysis of security and safety work scope of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016 and Tokyo 2021 Olympic Games.

3) Main objective 3: Comparative analysis of the security and safety budget of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016 and Tokyo 2021 Olympic Games.

4) Sub-objective: Providing future perspectives on security and safety within the project management of the Olympic Games.

The sample consist of six summer Olympic Games case studies covering the 21-year period: Security and safety of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016, Tokyo 2021 Olympic Games. Data collection includes open-source data collected from scientific articles, professional articles, policies and reports on governance, work scope and budget of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016 and Tokyo 2021 Olympic Games (table 1). Variables included the governance (security and safety structure of the Olympic Games),

work scope-related data (activities of the security and safety stakeholders) and the security-related budget for each case study.

Table 1: Case studies related sources

CASE STUDY	SOURCES
Sydney 2000	ASIO. 2000. Report to Parliament 1999-2000. Australian National Audit Office. 1998. Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games.
Athens 2004	Migdalovitz, C. 2004. Greece: Threat of Terrorism and Security at the Olympics. Congressional Research Service: Library of Congress. RS21833. Ministry of Public Order Press Office. 2004. Administration, co-ordination and control of Olympic security operations. Samatas, M. 2007. Security and Surveillance in the Athens 2004 Olympics - Some Lessons from a Troubled Story. International Criminal Justice Review. 17, 220-238. Toohey, K. & Taylor., T. 2007. Perceptions of Terrorism Threats at the 2004 Olympic Games: Implications for Sports Events. Journal of Sport and Tourism, 99-114.
Beijing 2008	Mulvenon, J. 2008. The Party Holds the Ring: Civil-Military Relations and Olympic Security. Mulvenon, China Leadership Monitor, 26. Yu, Y., Klauser, F. & Chan, G. 2009. Governing Security at the 2008 Beijing Olympics. The International Journal of the History of Sport 26, 3, 390-405.
London 2012	Home Office. 2011. London 2012 Olympic and Paralympic Safety and Security Strategy. UK Government, London. Houlihan, B., & Giulianotti, R. 2012. Politics and the London 2012 Olympics: the (in)security Games. International Affairs 88, 4, 701-717. House of Commons Home Affairs Committee Olympics Security Seventh Report of Session 2012-13. London 2012 Olympic and Paralympic Games Quarterly Report (2012, October).
Rio de Janeiro 2016	Bitencourt, L. 2011. The Security Challenges for the 2016 Rio de Janeiro Olympic Games. Western Hemisphere Security Analysis Center, 5. Halchin, L.E. & Rollins, J.W. 2016. The 2016 Olympic Games: Health, Security, Environmental, and Doping Issues. Library of Congress. Congressional Research Service. Winter, R. 2016. Cyber Risks During Events - Rio Olympics 2016. Technical report.
Tokyo 2021	Dion-Schwarz, C., Ryan, N., Thompson, J.A., Silfversten, E. & Paoli, G.A. 2018. Olympic-Caliber Cybersecurity Lessons for Safeguarding the 2020 Games and Other Major Events. RAND. Ilevbare, S.I. & McPherson, G. 2022. Understanding COVID-19: A Hybrid Threat and Its Impact on Sport Mega-Events. A Focus on Japan and the Tokyo 2020 Olympic Games. Frontiers in sports and active living, 4, 720591, 1-14. Sugiyama, K. 2020. Development of New Security Measures for the Tokyo Olympic & Paralympic Games and the Transformation of Public Space. Annals of the Association of Economic Geographers, 66, 1, 112-135. The Tokyo Organising Committee of the Olympic and Paralympic Games. 2021. Update to the Sustainability Pre-Games Report.

Data analysis includes comparative analysis of security and safety governance, work scope and the budget of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016 and Tokyo 2021 Olympic Games. The limitation of this research is the fact that certain security data were classified as confidential and therefore exclusively open-source data was used.

3 Results, comparative analysis and discussion

3.1 Comparative analysis of security and safety governance

Without a doubt, the Olympic Games are the largest international multi-sport event. The security and safety of the Olympic Games is constantly evolving, and at each subsequent Games it becomes more complex. Consequently, it occupies one of the largest shares in the total cost of organizing this mega popular event. For the security and safety purpose, Sydney 2000 deployed 5 000 police officers, 3 500 military officers and 7 000 contracted security staff. Only eight years later, Beijing organizers mentioned 92 500 people being involved in the direct security of the Games (that figure does not include an additional 100 000 regular soldiers and 290 000 civilian security volunteers). Within the overall project management, it is therefore important to organize effective Games security, which requires good governance, interdepartmental and international cooperation, thorough risk assessment, precise strategy, clearly defined work scope and responsibilities. Sanan (1996) notes that Olympic security should be both comprehensive and unobtrusive, and posits this as one of the defining characteristics of Olympic security. For this purpose, good governance and proper management are important. The International Olympic Committee stipulates that security issues are the sole responsibility of the host city (Bellavita, 2007). Although the responsibility for security is entrusted to the host of the Olympic Games, the evolution of security and safety indicates a transition from a domicile approach to international and multi-agency cooperation. After the establishing a seven-nation Olympic Advisory Group from Australia, France, Germany, Israel, Spain, the United Kingdom and the United States for advisory purposes of the Athens Olympics 2004, the international cooperation becomes unavoidable. Four years later, Beijing invited experts from 75 security agencies from 12 countries, including Greece, Canada, USA, Germany, France, UK, Israel and Russia, to collaborate for the 2008 Olympics securitization. Although the domicile authorities of the Games are the main bearers of security and safety, in operational terms (especially with risk evolution) security cannot be imagined without the cooperation and capacity (human and technological) of different national organizations, private companies and volunteers, as an unavoidable stakeholder of the Olympic Games. Thus, with each new Olympic Games, the number of bodies and structural units involved increases, the number of security personnel increases, as does the total security expenditure. Broader processes of transnational and multi-agency collaboration and knowledge transfer are also centrally implicated in this process (Spaaij, 2016). According to the Oquirrh Institute (2003) each agency is inevitably concerned about their specific responsibility and views their task as the highest priority, especially if it can publicly be associated with their agency. Different agencies are going to have their own interests, their own agenda and, to a certain degree, their own internal culture which inhibits spontaneous cooperation. Additionally, jurisdictional issues lead to hierarchy and power-sharing disputes at even at the most basic level of security planning. Inter-agency rivalry does exist, people do not cooperate as they should, and information is not freely exchanged. If all goes well, the extent of this is never an issue but in the event of a crisis or high-pressure situation, there are no guarantees that the various agencies and departments can avoid resorting to an individualistic mindset (Oquirrh Institute, 2003). However, a comparison of case studies shows that clear responsibility and hierarchy are necessary. The host of the Games designates the existing or newly established body as the main organization responsible for security, and includes a complex stakeholder's matrix: police, military, intelligence, fire unites, air force, private security staff, volunteers, etc. In advisory and operational terms, there is a growing emphasis on international cooperation with those who gained the know-how in securing the Olympic Games. Institutional security networks are platforms for inter-agency coordination (Brodeur and Dupont, 2008). These networks may include local, national and

international actors or agents and, in the context of sports events, public and private actors (Palmer and Whelan, 2014). Virtual networks, in addition, provide the technical infrastructure enabling the communication and exchange of data and information between security agencies or agents (Dupont, 2004). The generation of post-9/11 uncertainties has further escalated the scale, intensity and scope of Olympic security practices, which both express and extend contemporary developments in global security governance. The Olympics are discursively constructed as "spaces of exception" wherein aggressive security and surveillance measures are justified to mitigate and prevent any potential or actual security risk (Boyle, 2012; MacDonald and Hunter, 2013). According to Krieger (2019) the Olympic stakeholders' security fears rose dramatically due to international terror threats. Without question, the anti-terror operations required the biggest share of the ever-increasing security budget of Olympic hosts.

3.2 Comparative analysis of security and safety work scope

The comparison of case studies shows the evolution of risks or their complexity. Despite the increased number of risks over time, as well as risks that were not particularly focused in Sydney 2000, and are now an integral part of security preparations for the Games (e.g., cybersecurity), terrorism holds firmly first in the overall security risk assessment of the Olympics. The identification of terrorism as a major threat to the Olympics is reflective of what Wæver (1995) have called securitization: the process by which an issue, having been labelled an existential threat, is moved out of the sphere of normal politics into the realm of emergency politics, where states can control and deal with it without the normal (democratic) rules and regulations of policy-making. Nevertheless, fears of terror remain a constant feature in the preparation and staging phases and lead to major challenges for event organizers and governing bodies of sport alike (Krieger, 2019). Fussey (2010) notes the complexity of determining what constitutes Olympic-related terrorism by pointing to complicating factors such as when a terrorist attack takes place in a host nation in the run-up to or during the Olympic Games without an apparent connection to the event, yet with considerable impact on Olympic security planning. Mass gatherings, pre-known dates of matches, high concentration of emotions, fun, carefreeness and achieving publicity without much expense make sports facilities attractive soft targets of terrorist attacks (Leško, 2018). Although large investments in security in terms of counter-terrorism measures during the past six Games have enabled no major terrorist incident to occur, terrorism remains the biggest threat due to the fact that terrorism is significantly cheaper than counter-terrorism. at the Olympics challenged. A key question is how the securitization of, and response to, terrorism can be balanced with democratic principles and respect for human rights and civil liberties (Spaaij, 2016). One of the challenges Olympic organizers facing is the need to balance the requirements of security and public safety with the festive and convivial nature of the Games (Spaaij, 2016). In addition, there is a growing focus on preventing and preventing cyber incidents and cyber terrorism, which is crucial in the overall risk assessment of the recent Olympics, especially because drastic damage to human victims and property damage can be done without the physical presence of perpetrators. Other potential threats, apart from the infrastructural risks of the collapse of sports and ancillary facilities, depending on the geolocation factors of the host, include domestic crime and violence, sabotage, natural hazards, epidemics (e.g., Zika virus), pandemics (SARS-CoV-2), etc. Planning Olympic security is a formidable task in part due to three challenges: logistical issues, interagency cooperation and a reliance on volunteers (Zekulin, 2009). The distance between the two main venues and creation of a third zone between them stretches limited resources, the number of agencies involved and their proven history of limited cooperation and coordination, and a documented shortage of volunteers may all affect security in some way (Zekulin, 2009). In the context of security, the problem of a sufficient number of trained security staff, i.e., the challenge of training and arranging volunteers, remains one of the main preoccupations of those responsible for the safety and security of the Olympic Games. The G4S-related issue for the London Olympics 2012 further confirms that fact.

An additional concern is the public protest over the high costs of hosting the Games, as well as over securitization or extensive surveillance methods at the expense of restrictions on personal liberties. Anti-terrorist measures of a ring of steel include physical and technical control of persons and vehicles

entering and leaving the city, fortification measures, physical and technical protection of vital facilities with fortification control of access to facilities, traffic regulation in the city with the introduction of red routes (risky roads where detention is prohibited), strengthening different types of security forces (military, police, special forces) and their visibility, extensive installation of digital video surveillance (Bilandžić and Leško, 2019). Many internationally renowned companies have played an important role in providing security support to the Olympics, public-private partnerships as well as outsourcing are becoming an integral part of security and safety of the Olympic Games. In terms of technology, quality communication devices, CCTV or modern tech like NEC's or Hitachi's system that can check up to 1 200 people per hour, have become indispensable in maintaining the Games security. Although, for example, the C4I integrative system was marked as a failure in Athens 2004 (Samatas, 2014). A new digital era, in addition to all the positive impacts on society, has also contributed to complicating security risks among the Olympics. The Olympic Cyber Coordination Team, the first "Olympic CERT" was established for the London 2012 and played one of the more important roles in the overall security for the Games that followed, as well as in their security budgets. Terms like (Spear) Phishing, Whaling, Vishing, DDoS, Malware or Ransomware that have not been well known to the general public twenty years ago, are an integral part of the risks of the recent Olympic Games. In the public health domain, epidemic like Zika virus in Brazil or pandemic like SARS-CoV-2 that hit the whole world, and thus the Tokyo Olympics, are considered as additional safety concern for those major sporting events. Moreover, Games in Tokyo have been postponed for one year for that reason.

3.3 Comparative analysis of security and safety budget

Over the period from 2000 to 2021, the Olympics did not record a major terrorist or cyber incident. In the context of minor incidents, as well as those prevented, deterred or prevented, it is ungrateful to speak respecting the nature of the security profession, which for multiple reasons classifies some of them as confidential and does not reach the public. The security and safety budget of the Olympic Games has been multiplied compared to the period of 20-30 years ago. After Sydney 2000 it stopped counting in millions rather than billions USD. The cost eruptions as a result of safety operations have led to new "fears" on staging the Olympic Games. Comparing the observed period from 2000 to 2021, the security budget of the Olympic Games was: Sydney 2000: 250 million USD; Athens 2004: 1.5-1.6 billion USD; Beijing 2008: 6.5 billion USD; London 2012: 3.1 billion USD; Rio de Janeiro 2016: 895 million USD (a significant part of the funds for security infrastructure was invested two years before for the World Cup); Tokyo 2021: initially estimated the security budget at about 900 million USD. Later on, another 900 million USD was estimated to be spent on measures to stop the spread of SARS-CoV-2. This is due to the complexity of security and safety risks, the development of sophisticated and expensive technology, the growing number of required security staff, as well as a certain share of support from other countries. Security investments are not sustainable and they do not produce any future economic revenues. However, they are indispensable to stage mega sport events in the present day and constitute a key concern for a sport organization such as the IOC already during the bidding process (Houlihan and Giulianotti, 2012). As such, the Olympics, like other major sports events, serve as an opportunity for the authorities to introduce security measures that would be more difficult to justify in normal circumstances (Bennett and Haggerty, 2011). It is broadly agreed that Olympic security arrangements can endure long after the event is over. Post-event security legacies are now a strategic issue in Olympic security planning. The intended and unanticipated security legacies are multifaceted. In addition to technological (for example biometric facial recognition), informational and knowledge legacies, they include the endurance of attitudes about security and surveillance whereby the Olympic 'state of exception' can become normalized (Bennett and Haggerty, 2011).

4 Future perspectives

Looking into the future, it should be said that the further Olympic Games were awarded to the rich cities (countries) of the western world. Paris will host the Olympics in 2024, Los Angeles in 2028. This is emphasized especially from the domain of terrorism. In modern times, France has been the

scene of devastating terrorist attacks, and the American 9/11 marked a kind of turning point in the general understanding and fight against terrorism. The most capable terrorist organizations do not hide their hostile aspirations towards western goals, especially those that have actively intervened against those organizations and their goals in recent times. Knowing the fact of the capacity of Russian hackers and their recorded hacking attacks in the context of the Olympics, amid new rigorous sanctions against Russian and Belarusian athletes for Russia's invasion of Ukraine, it will be very challenging to protect the cyberspace of the Olympics. Of course, if these sanctions last a longer period of time. According to IOC (2017), Paris 2024 has proposed comprehensive safety and security measures, appropriate to host the Games and consistent with the relevant guarantees. The French Government has committed to provide all necessary support to deliver safe and peaceful Games. Security for the Games would benefit from recent refinements in security-agency roles and capabilities, the centralization of intelligence capabilities and other positive responses to recent security challenges in France. The current security threat level across the Paris region is classified as "high" by French authorities. The proposed security measures for 2024 would reduce the risk level in Olympic Venues to "very low" and the Olympic Route Network to "low", thereby providing a safe environment for Games' constituents. Concurrently, the authorities estimate the risk in the public domain would be "medium". There is low risk of safety issues related to weather or natural disasters. Security is marked one of the main budget-related challenge. Atos becomes the exclusive Official Cybersecurity Services and Operations Supporter for the event. To digitally secure the Olympics, Atos will provide cybersecurity products and solutions, manage cybersecurity planning and preparation and cybersecurity operations. As a leader in secure and decarbonized digital, Atos will also commit to the provision of decarbonized solutions to support Paris 2024 in their aim to create a sustainable experience for all stakeholders (Atos.net, 2021). In the provision of cybersecurity solutions to Paris 2024, amongst other services, Atos (Atos.net, 2021) will be delivering: Security Operations Center; Security Response Orchestration, Automation and Coordination; Security Information and Event Management; Emergency response team and the management of cybersecurity incidents and threat hunting; Advanced Data Leakage Protection; Online fraud prevention including behavioral analysis based on Artificial Intelligence; Privileged access management. The initially estimated total budget of the Paris 2024 Olympics is 7.7 billion $, of which a high share is expected to be spent on security and safety as France itself is one of the more common targets of terrorism in Europe, while hosting the largest sporting event additionally complicates security risks.

According to the IOC (2017) Los Angeles 2024 has proposed comprehensive safety and security measures, appropriate to host the Games and consistent with the relevant guarantees. The US Department of Homeland Security has guaranteed the Games would receive National Special Security Event (NSSE) designation, which would provide world-leading security expertise, capabilities and resources to augment existing arrangements. Under NSSE, the US Secret Service would be the lead security agency, supported by numerous other federal agencies, including the FBI and the Federal Emergency Management Agency. The current security threat level across the Los Angeles region is classified between "low" and "medium" by relevant authorities. The proposed security measures for 2024 would reduce the risk level in Olympic venues to "very low", with "low" for the Olympic Route Network, thereby providing a safe environment for Games constituents. Concurrently, the authorities estimate that the risk in the public domain would be "low" or potentially "very low". There is low risk of safety issues related to weather. Los Angeles is in a seismic zone, although this matter is addressed in all aspects of construction and infrastructure. LA 2024 has relatively low expectation of government support for operational expenses; these are primarily in the areas of transport and security.

Taking into account case studies and additional literature (theoretical, empirical and policy), the following are summarized future perspectives in the form of recommendations for optimal security and safety for the further Olympic Games.

1) The formal institutional set-up of security is crucial;

2) Due to the large number of organizations/departments/units as stakeholders (police, military, intelligence, private security volunteers, etc.), it is important to precisely determine the jurisdiction, work scope and responsibility, including formalized chains of command;

3) Games Intelligence Center is an important integral part of the Games-related security system;

4) In order to reduce multi-agency rivalry, timely joint educational and practical trust building campaigns are recommended;

5) The advices of other countries that have the "know-how" in securing the Olympics are vital;

6) Considering the use of sophisticated AI-based predicting software on both physical and cyber security which, in synergy with the knowledge and experience of security professionals, can be useful in terms of risk assessment and cost optimization in security planning of the event;

7) Risk Assessment is a necessary starting point in security preparation (identifying potential threats; assessment of potential damage from such threats; estimating the probability for each individual threat; assessment of costs and activities to combat threats);

8) Security and safety strategy is the core document, made on the basis of a risk assessment;

9) Counter-terrorism strategies are an integral part of the security preparations for the Olympic Games;

10) Each venue should have a corresponding security action plan;

11) Volunteers are an integral part of the overall security ecosystem;

12) Timely training of security staff, including test events and other types of simulation scenarios are necessary in the preparation of staff. Test events are important both for testing security procedures and testing personnel capability for acting in real time stress situations;

13) The accreditation and zoning system is at its closest to security and safety. Zoning is necessary for access control of participants, according to their particular purpose at the event;

14) Despite disputes over the restriction of human rights and liberties, surveillance is an essential method of maintaining security at the Olympics;

15) The highest quality detection, communication and integration technology must be used;

16) Although challenging in the context of securitization, it is important to find the optimal balance between the visibility of security staff and the positive experience of participants and spectators;

17) Special attention on the information security (behavioral, physical, personnel and technical aspects);

18) The CERT has to be an integral part of the Games-related security. Special attention to cyberspace security includes regular audits, using Access Control List (ACL), effective DDoS Protection Essentials (Hybrid DDoS Protection, Behavioral-Based Detection, etc.);

19) Lines of communication among security personnel must be clearly defined;

20) The risk management system must be clearly defined and effective;

21) Post-Event activities include evaluations, reporting and providing lesson learned;

22) Significant investments can be justified by long-term legacy in terms of urban development, personnel, technology, governmental policies, etc.

5 Conclusions

Security is a necessary constitutive element of society. Expanding the range of security risks led that security studies are in evolutionary continuity. Contemporary studies show the relevance of examining sports from a security and safety perspective. Terrorism affected various social phenomena, including sport as an integral factor of society. This is especially confirmed by empirical data of the Olympic Games, one of the most watched events on the globally basis and events that are without a doubt, one of the world's largest peacetime security challenges, through which countries (and community) achieve long-term legacy in the form of infrastructural, technical and personnel security achievements. Security and safety became one of the most important (and the most expensive) parts within the

project management of the Olympic Games. The Olympic Games require one of the most complex mass event-related security operations in the world. Alongside risk evolution, in terms of security and safety of major sporting events as mass gatherings, each of the following Olympic Games are more complex, which indicates the general failure of society to gradually make life safer. This confirms the basic determinants of security studies as such, which are constantly expanding and deepening. Defense against terrorism is significantly more expensive than terrorism itself. Although it is suppressed by large investments in security, terrorism remains the greatest threat to the Olympics due to the scale of direct (human fatalities and property damage) and indirect effects (public fear and anxiety). Cyber-attacks, in which damage can be done without the physical presence of the perpetrator are becoming an extremely threat to the Olympics. Due to the drastic increase in the security capacity of the Olympic Games, no realized major security incidents were recorded from 2000 to 2021. In terms of governance, evolution from domicile to international multi-agency cooperation and evolution of the number of stakeholders involved, suggest that each subsequent Olympic Games are more complex. In terms of sustainability, although the security budget occupies a significant share of the total organizational budget of the games (post-9/11 security budget is no longer measured in millions but in billions USD), those investments can be justified by long-term legacy in terms of urban development, personnel, technology, governmental policies, etc. Finally, empirical learning based on case studies has proved important in the security preparation of the Olympic Games, so this study will contribute to creating a broader picture in the context of the security of the Olympic Games, with an emphasis on governance, work scope and budget. Further research should address the methods to optimize security measures against restrictions of human rights and liberties. In addition to deepening theoretical and empirical studies of counterterrorism, further research on prevention of inter-agency rivalry as well as prevention of cyber-attacks on the Olympic Games and their actors is recommended.

References

ASIO. 2000. *Report to Parliament 1999-2000.*

Atos.net. 2021. *Atos becomes the Official Cybersecurity Services and Operations Supporter of the Olympic and Paralympic Games Paris 2024*. https://atos.net/wp-content/uploads/2021/04/Atos-becomes-the-Official-Cybersecurity-Services-and-Operations-Supporter-of-the-Olympic-and-Paralympic-Games-Paris-2024_P24.pdf. Accessed 23rg March 2022.

Australian National Audit Office. 1998. *Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games*.

Bellavita, C. 2007. "Changing Homeland Security: A Strategic Logic of Special Event Security." Homeland Security Affairs, 1-23.

Bennett, C. J., & Haggerty, K. D. 2011. *Security games: Surveillance and control at mega-events*. A Glass House book. Abingdon, Oxon, New York: Routledge.

Bilandžić, M. & Leško, L. 2019. *Sport i nacionalna sigurnost [Sport and national security]*. Zagreb: Despot infinitus.

Bilandžić, M. 2014. *Sjeme zla: uvod u studije terorizma*. Zagreb: Despot infinitus.

Bitencourt, L. 2011. *The Security Challenges for the 2016 Rio de Janeiro Olympic Games.* Western Hemisphere Security Analysis Center, 5.

Bourbeau, P. 2015. *A multidisciplinary dialogue on security*. In: Bourbeau, P. 2015. (ed.) Security: Dialogue across Disciplines. Cambridge: Cambridge University Press.

Boyle, P.J. 2012. *Securing the Olympic Games*. In: Pete Fussey and Jon Coaffee, Balancing Local and Global Security Leitmotifs: Counter-Terrorism and the Spectacle of Sporting Mega-Events, International Review for the Sociology of Sport 47, 3, 268-85.

Brodeur, J.-P. & Dupont, B. 2008. *Introductory Essay: The Role of Knowledge and Networks in Policing*. In: The Handbook of Knowledge-Based Policing: Current Conceptions and Future Directions, ed. T. Williamson, 9-36. West Sussex: John Wiley & Sons.

Buzan, B. & Hansen L. 2009. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Coakley, J. 2009. *Sports in Society: Issues and Controversies (10th edition)*. New York: McGraw-Hill.

Dion-Schwarz, C., Ryan, N., Thompson, J.A., Silfversten, E. & Paoli, G.A. 2018. *Olympic-Caliber Cybersecurity Lessons for Safeguarding the 2020 Games and Other Major Events*. RAND.

Dupont, B. 2004. *Security in the Age of Networks*. Policing & Society 14, 1, 76-91.

Fussey, P. 2010. *Terrorist threats to the Olympics, 1972-2016*. Routledge 1st Edition.

Giulianotti, R. & Klauser, F. 2012. *Sport mega-events and 'terrorism': A critical analysis*. International Review for the Sociology of Sport 47, 3, 307-23.

Halchin, L.E. & Rollins, J.W. 2016. *The 2016 Olympic Games: Health, Security, Environmental, and Doping Issues*. Library of Congress. Congressional Research Service.

Home Office. 2011. *London 2012 Olympic and Paralympic Safety and Security Strategy*. UK Government, London. http://www.homeoffice.gov.uk/counter-terrorism/2012-olympic-games/ (accessed 30th March 2022)

Houlihan, B., & Giulianotti, R. 2012. *Politics and the London 2012 Olympics: the (in)security Games*. International Affairs 88, 4, 701-717.

House of Commons Home Affairs Committee Olympics Security Seventh Report of Session 2012-13. https://publications.parliament.uk/pa/cm201213/cmselect/cmhaff/531/531.pdf Accessed 15th March 2022.

Ilevbare, S.I. & McPherson, G. 2022. *Understanding COVID-19: A Hybrid Threat and Its Impact on Sport Mega-Events. A Focus on Japan and the Tokyo 2020 Olympic Games*. Frontiers in sports and active living, 4, 720591, 1-14.

IOC Candidature Acceptance Working Group. 2008. *Games of The XXXI Olympiad 2016 Working Group Report*.

IOC. 2015. *Olympic Games Framework: Produced for the 2024 Olympic Games*.

IOC. 2017. *Report of the IOC 2024 Evaluation Commission*. https://stillmed.olympic.org/media/Document%20Library/OlympicOrg/Documents/Host-City-Elections/XXXIII-Olympiad-2024/Report-IOC-Evaluation-Commission-2024-low-resolution.pdf. Accessed 23rd March 2022.

Krieger, J. 2019. *How Fears Changed the Games: Of Terror, Security and Costs*. In: Dark Sides of Sport (eds. Krieger, J., Wassong, S.), Common Ground Publishing, 57-72.

Leško, L. 2018. *Teroristički napadi na sportske objekte od 1970-ih do 2017. godine: od selektivne do masovne destrukcije. [Terrorist attacks on sports facilities from the 1970's until 2017: from selective to mass destruction]*, Polemos, 21, 42, 127-162.

London 2012 Olympic and Paralympic Games Quarterly Report (2012, October). https://www.gov.uk/government/publications/london-2012-olympic-and-paralympic-games-quarterly-report-october-2012. Accessed 15th March 2022.

MacDonald, M. & Hunter, D. 2013. *The Discourse of Olympic Security: London 2012*. Discourse & Society 24, 1, 66-88.

Migdalovitz, C. 2004. *Greece: Threat of Terrorism and Security at the Olympics*. Congressional Research Service: Library of Congress. RS21833.

Ministry of Public Order Press Office. 2004. *Administration, co-ordination and control of Olympic security operations.*

Mulvenon, J. 2008. *The Party Holds the Ring: Civil-Military Relations and Olympic Security*. Mulvenon, China Leadership Monitor, 26.

Noble, R. 2007. *International Conference on Security Cooperation for 2008 Beijing Olympic Games*. Interpol. http://www.interpol.int/Public/ICPO/speeches/Beijing20070910.asp (accessed 20th March 2022).

Oquirrh Institute. 2003. *The 2002 Olympic Winter Games Security Lessons Applied to Homeland Security*. 2002 Olympic Security Review Conference.

Palmer, D. & Whelan, C. 2014. *Policing and Networks in the Field of Counterterrorism*. In: Examining Political Violence: Studies of Terrorism, Counterterrorism, and Internal War, eds D. Lowe, A. Turk, and D.K. Das, 145-166. Boca Raton: CRC Press.

Samatas, M. 2007. *Security and Surveillance in the Athens 2004 Olympics - Some Lessons from a Troubled Story*. International Criminal Justice Review. 17, 220-238.

Samatas, M. 2014. *The «Super-Panopticon» Scandal of The Athens 2004 Olympics and its Legacy*. Athens: Pella.

Sanan, G. 1996. *Olympic Security Operations 1972-94*. In: Alan Thompson (ed.), Terrorism and the 2000 Olympics. Canberra: Australian Defence Studies Centre, 35.

Savitch, H. 2003. *Does 9-11 Portend a New Paradigm for Cities?* Urban Affairs Review 39, 1, 103-127.

Spaaij, R. 2016. *Terrorism and Security at the Olympics: Empirical Trends and Evolving Research Agendas*. The International Journal of the History of Sport 33, 4, 451-68.

Sugiyama, K. 2020. *Development of New Security Measures for the Tokyo Olympic & Paralympic Games and the Transformation of Public Space*. Annals of the Association of Economic Geographers, 66, 1, 112-135.

The Tokyo Organising Committee of the Olympic and Paralympic Games. 2021. *Update to the Sustainability Pre-Games Report*.

Toohey, K. & Taylor., T. 2007. *Perceptions of Terrorism Threats at the 2004 Olympic Games: Implications for Sports Events*. Journal of Sport and Tourism, 99-114.

Wæver, O. 1995. *Securitization and Desecuritization*. In: Ronnie D. Lipschutz (ed.), On Security (New York: Columbia University Press), 46-86.

Walsh, J. P. 2016. *Moral panics by design: The case of terrorism*. Current Sociology 1, 5, 1-20.

Winter, R. 2016. *Cyber Risks During Events - Rio Olympics 2016. Technical report*. https://www.researchgate.net/publication/312038398_Cyber_Risks_During_Events_-_Rio_Olympics_2016

Yu, Y., Klauser, F. & Chan, G. 2009. *Governing Security at the 2008 Beijing Olympics*. The International Journal of the History of Sport 26, 3, 390-405.

Zekulin, M. 2009. *Olympic Security: Assessing the Risk of Terrorism at the 2010 Vancouver Winter Games*. Journal of Military and Strategic Studies, 12, 1.