# GOVERNANCE, WORK SCOPE AND BUDGET FOR SECURITY AND SAFETY WITHIN THE PROJECT MANAGEMENT OF THE SUMMER OLYMPIC GAMES FROM SYDNEY 2000 TO TOKYO 2021: COMPARATIVE ANALYSIS AND FUTURE PERSPECTIVES

by

Luka Leško, Ph. D.

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

JUNE, 2022

GOVERNANCE, WORK SCOPE AND BUDGET FOR SECURITY AND SAFETY WITHIN THE PROJECT MANAGEMENT OF THE SUMMER OLYMPIC GAMES FROM SYDNEY 2000 TO TOKYO 2021: COMPARATIVE ANALYSIS AND FUTURE PERSPECTIVES

by

Luka Leško, Ph. D.

APPROVED BY

Anna Provodnikova

Anna Provodnikova, Ph. D., Chair

Minja Bolešnikov, Ph. D., Committee Member

Mario Silić, Ph. D., Committee Member

RECEIVED AND APPROVED BY:

Dino Kolak

Dino Kolak, Admission Director

## Dedication

*I dedicate the dissertation to everyone in the academic and professional community who will benefit from its content.*

**Acknowledgements**

*First of all, I would like to thank the College of Occupational Safety and Health for recognizing my potential by investing further into my business education. I believe in mutual long-term benefit.*

*Special thanks to the mentor Mario Silic, Ph. D., whose expertise and experience contributed to the quality of this dissertation, as well as to the members of the evaluating committee for the time invested in the review of the dissertation.*

*Special thanks to Mirko Bilandzic, Ph. D., for all the time invested in our friendly conversations and joint scientific work in the field of security.*

ABSTRACT

GOVERNANCE, WORK SCOPE AND BUDGET FOR SECURITY AND SAFETY WITHIN THE PROJECT MANAGEMENT OF THE SUMMER OLYMPIC GAMES FROM SYDNEY 2000 TO TOKYO 2021: COMPARATIVE ANALYSIS AND FUTURE PERSPECTIVES

Luka Leško, Ph. D.
2022

Dissertation Chair: Mario Silic, Ph. D.

The Olympic Games require one of the most complex mass event-related security operations in the world. Security and safety became one of the most important (and the most expensive) parts within the project management of the Olympics. Using both theoretical and empirical knowledge, this research on governance, work scope and budget for security and safety within the project management of 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. Alongside risk evolution, 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 - constantly expanding and deepening. Counter-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. The evolution of risk has conditioned the CERT to be an indispensable part of the security preparation of the Olympics. Due to the drastic increase in the security capacity of the Olympics, 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. 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. 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 at the Olympic Games is recommended.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

17N - Revolutionary Organization 17 November
3C - Closed spaces, Crowded places, Close-contact settings
ABIN - Brazilian Intelligence Agency
ACL - Access Control List
ANN - Artificial Neural Networks
ASIO - Australian Security Intelligence Organisation
ASIS - American Society for Industrial Security
ATM - automated teller machine
AWAC - Airborne Warning and Control System
C4I - command, control, communications, computers, and intelligence /integration/
CCTV - Closed-circuit television
CDC - Centers for Disease Control and Prevention
CERT - Computer Emergency Response Team
CIA - Central Intelligence Agency (US)
CIJ - Games Intelligence Center
DDoS - distributed denial-of-service
DGA - domain-generating algorithms
DOD - Department of Defense
ETA - Euskadi Ta Askatasuna (Basque separatist organization in Spain that used terrorism in its campaign for an independent Basque state)
FBI - Federal Bureau of Investigation
FEMA - The Federal Emergency Management Agency is an agency of the United States Department of Homeland Security
FIFA - Fédération Internationale de Football Association (International Federation of Association Football).
G4S - British multinational private security company headquartered in London
GBP - Great Britain pound
GRU - Glavnoye Razvedyvatelnoye Upravlenie (The Main Directorate of the General Staff of the Armed Forces of the Russian Federation)
IAEA - International Atomic Energy Association
IOC - International Olympic Committee
IoT – Internet of things
IP - Internet Protocol
ISIS - Islamic State (Islamic State of Iraq and the Levant or the Islamic State of Iraq and Syria)
ISP - Internet service provider
MI5 - Military Intelligence, Section 5 (United Kingdom's domestic counter-intelligence and security agency)

MITM - In cryptography and computer security, a man-in-the-middle attack is a general term for when a perpetrator positions himself in a conversation between a user and an application.
NATO - North Atlantic Treaty Organization
NIS-EYP - Ethnikí Ypiresía Pliroforión (the National Intelligence Service is the national intelligence agency of Greece)
NOC - National Olympic Committee
NSSE - National Special Security Event
OAG - Olympic Advisory Group
OCOG - Host city's Organizing Committee for the Olympic Games
OG - Olympic Games (in this context, the term also includes the Paralympic Games)
OSAC - Overseas Security Advisory Council
OSAG - Olympic Security Advisory Group
OSB - Olympic Security Board
OSCT - Office for Security and Counter Terrorism
OSWC - Olympic Security Working Committee
OWASP - Open Web Application Security Project (online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security)
PAP - Chinese People's Armed Police Force
PII - Personally identifiable information (PII) is any data that could potentially identify a specific individual.
PIRA - Provisional Irish Republican Army
PLA - People's Liberation Army (armed forces of the People's Republic of China)
PM - Project management
PPP - Public-private partnerships
RAF - Royal Air Force is the United Kingdom's air and space force.
RFID - Radio frequency identification (wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to identify an object, animal or person)
SAC-PAV - Commonwealth/State Cooperation for Protection Against Violence
SDN - Software-defined networking
SPIN - Segmented, polycentric (ideologically) integrated networks
SPIS - Strategic Plan for Integrated Security
SQL - Structured Query Language (a domain-specific programming language used for managing data held in a relational database management system or for stream processing in a relational data stream management system)
TCMOR - Traffic Control and Monitoring Operations Room
UCLA - University of California, Los Angeles
UEFA - Union of European Football Associations
UN - United Nations
UOPSC - The Utah Olympic Public Safety Command
USD - US dollar
VPN - virtual private network

WADA - World Anti-Doping Agency
WHO - World Health Organization
XML - Extensible Markup Language

# CHAPTER I:

# INTRODUCTION

The Olympic Games require one of the most complex mass event-related security operations in the world. The problem of emphasis of academic research on major sporting events mainly in the field of sporting achievements, i.e., the lack of comparative research on the development of the concept of 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. The fundamental aim of this research is comparative analysis of governance, work scope and budget of the security and safety within the project management of the Sydney 2000, Athens 2004, Beijing 2008, London 2012, Rio de Janeiro 2016 and Tokyo 2021 Olympic Games in order to examine the conceptual development and improvement of security and safety over the last six summer Olympic Games. Also, this research provides future perspectives on security and safety within the project management of the Olympic Games. Research expands knowledge and future perspectives in the field of expanding the security risks of the Olympic Games as one of the world's largest international events and ways to deal with them through the prism of governance and work scope, accompanied by total expenditure. 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.

### 1.1 Security: Theoretical background

Security is a necessary constitutive element of society. As a public good and non-exclusive value, security has a significant impact on social, economic and political processes (Loader and Walker, 2007). It is a specific construct compared to other fields of science. Security is socially constructed, it has different meanings for different actors (Malik, 2015). Starting from the Latin root of the word (lat. secures - carefree), security comes from social processes that reduce risk and improve normality, predictability, mutual calm and self-confidence (Risley, 2006). In the objective sense, it measures the absence of threats to acquired values, and in the subjective sense, the absence of fear that such values will be endangered (Wolfers, 1962). Within academic and professional communities, an almost undivided view has been reached that the study of security is dominated by three theoretical approaches: realism, liberalism and constructivism (Croft, 2008). In the theoretical-conceptual sense, the end of the Cold War turmoil marked the entry of constructivist perspectives into security studies. Constructivist theories are based on various factors influencing the formation of identity (socialization, interaction, learning between countries), which determines the behavior of countries in two dimensions: how the country sees itself and how other countries see it (Frazier and Stewart-Ingersoll, 2010). Constructivists believe that identity is a central element in the construction of security (McDonald, 2008; Neumann, 2010). At the same time, social conflicts are always marked by an opposing interest and identity dimension (Sen, 2007). Security studies do not fully meet the dimensions that sociologists of science expect from an established scientific field. The concept of security is not a stable and fixed object of rational knowledge, but is socially

constructed (Bilandžić, 2014). According to Bilandžić (2014) security studies are located between several different disciplinary approaches, it is a type of knowledge production that follows not only the logic of academic/scientific work but also the logic and requirements of the national establishment and public expectations. History, but also the recent period, indicates 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). Therefore, security is not a binary model (secure-insecure), but a future state of existence that is continuously achieved through risk management and routine supervision practices, which reinforces the daily ubiquity of security (Bourbeau et al., 2015). Significant issue explored in the literature is the demarcation between the concepts of security and safety (Jore, 2019). Numerous scholars, including Reniers et al. (2011), Reniers and Audenaert (2014), expressed a common opinion that security refers to protection from intentional crimes, such as terrorism and cyberattacks[1], whereas safety covers defence from occasional and unexpected events (Boholm et al., 2015; Jore and Egeli, 2015). As an example, infrastructural incidents should be accounted for by safety measures, whereas deliberately conducted terrorism and sabotage are in the area of security measures attention (Randall, 2008).

[1] Malicious attempts and acts of damaging, stealing data, and/or disrupting the digital life (Chen et al., 2017). In this context, it should be noted that cyber-attack and cyberterrorism are not synonymous. A cyber-attack is aimed at a computer, information system, or computer network, with not necessarily a terrorist motive.

## 1.2 Terrorism: Theoretical background

Security is a structural element of the survival and action of the individual, society, country and the international order, one of the basic human needs (Bilandžić and Mikulić, 2007). It is therefore important to study phenomena like terrorism, that threaten security. Terrorism is the product and result of a multifaceted combination of a number of factors: historical, political, social, cultural, ideological, religious, economic and psychological (Friedman, 2003). In the 14th century, the term terror entered the French dictionary, and two centuries later into the English dictionary, according to which the term terrorism was created (from the Latin word *terrere, terreo* - to lead someone to anxiety through great fear). Decades of efforts by science and the profession to reach consensus on the definition of terrorism have not succeeded yet. Schmid (2004) mentioned four reasons which, in his opinion, are the reason for this:

1) Terrorism is a controversial concept. The political, legal, as well as the views of the social sciences and the general public are largely divergent;
2) The issue of definition is related to (de)legitimization and criminalization;
3) There are several types of terrorism with different forms and manifestations;
4) The term has undergone numerous changes of meaning in more than 200 years of its existence.

This is supported by the fact that the US administration uses more than twenty definitions, with definitions changing every three to four years within individual departments (Schmid, 2011). In a broader sense, terrorism is the use of violence (terror) to

achieve political goals, and frequency analysis of existing definitions indicates that they are dominated by the following words: violence/use of force, political element, fear/terror, threat and psychological effects (Bilandžić, 2014). In counter-terrorism activities, countries use a variety of instruments: police, criminal law, military, intelligence, political, civil, sometimes amnesties to end terrorist activity (Jones and Libicki, 2008), but the fight against terrorism often requires international cooperation. Security compromisers have opportunities for faster mobility of people, funds and weapons than countries organizations that are bound by international regulations (Shiraz and Aldrich, 2013), with soft targets being an increasingly common choice of security threats against hard-defended targets such as military facilities, embassies, etc. Additionally, the exponential growth of cyberspace in the modern era has multiplied potential threats (Clemente, 2013).

Terrorist organizations are well-organized, managerial members are often highly educated, they renounce personal identity by taking new names, and they prepare and carry out operations secretly, which makes defense difficult. They have a defined structure and decision-making processes, recognized leaders in positions of formal authority, develop functionally differentiated roles and collective goals that they achieve as a unity with collective responsibility (Gunaratna and Oreg, 2010). Traditional ones are strictly hierarchical, while modern terrorist organizations have a more decentralized network structure (Scott, 2009), which can be chain, star or all-channel type, and often function as segmented polycentric ideologically integrated networks or SPIN (Arquilla and Ronfeldt, 2001). Apart from Al-Qaeda (translated as *the base*), the most famous example of a decentralized network structure linked to various terrorist organizations, other

organizations are often interconnected. They often have units for political or military issues, information, planning and preparation of operations, intelligence, counterintelligence and security operations, logistics, training, financing and technology, and a selective accession process. For example, the Al-Qaeda Manual (2000), found by Manchester police in 2000 on a terrorist's computer, described the organization and tasks of the military wing, the required qualifications and characteristics of members, instructions for counterfeiting money and documents, instructions for espionage and encrypted communication, attack methodology, etc. Every terrorist organization has its own value structure and specific modus operandi. Thus, their motivation becomes rational and can be observed within the concept of axiological rationality (Tosini, 2007). Despite different approaches, experts agree that there is no specific type of person who becomes a terrorist (Furedi, 2009; Intriligator, 2010), which further complicates the prevention of terrorist attacks. Interdisciplinary research has almost eliminated the psychopathological dimensions of terrorists (Bilandžić, 2014).

Terrorists are aware of the work of national intelligence agencies, so the number of members of a terrorist organization is often limited to carrying out attacks until just before the attack, with strict control over the disclosure of information in mutual, often encrypted communication (Pillar, 2011). Accordingly, breaking even the highest levels of their management does not necessarily mean disclosing information about local cells, especially in decentralized organizations (Bilandžić, 2014). Also, the value of quality information in the field of terrorism is short-lived, which requires timely responses (Byman, 2014). Terrorists typically attack when they are fully confident in the effectiveness of an act, so

even less information gathered from the national intelligence may lead them to give up (Clarke, 2004). Although Gerges (2011) found that the US National Security Agency (NSA) collects about 1.7 billion records of controlled communications daily, in reality the agencies are often faced with a shortage of key information about terrorist networks (Gerecht, 2001). This is best confirmed by the fact that CIA's estimates in August 2001 indicated possible Al-Qaeda attacks on US interests and targets abroad, but not on US soil (Bilandžić, 2014). In the real world of intelligence agencies, great discoveries are the result of hard work, slow gathering of facts, each of which seems ambiguous, but as the whole helps to make assumptions (Panetta and Newton, 2014). One of the most demanding challenges of counter-terrorism is in detecting attacks of the so-called lone-wolves, who may or may not be members of a terrorist organization, and who generally do not leave a trace of communication during the preparation of the attack (Bilandžić and Leško, 2019). They can independently carry out a terrorist act, inciting publicly announced calls by terrorist groups to commit an attack. These people do not have to be directly connected to terrorist organizations and they can self-radicalize through the internet and social networks, making it difficult for detection. An aggravating circumstance in the defense against terrorism is both the innovative and the changing modus operandi, replacing one form with another. What used to be dominated by assassinations and hijackings, hit and run tactics, has been replaced in recent years by suicide bombings, for example. In this context, given the strengthening of security measures at the airports, terrorists are forced to change targets, which include subways, squares, tourist destinations, sports facilities, theaters, nightclubs, etc. (Bilandžić, 2014). According to the US National Counterterrorism Strategy (The White

House, 2018), improving the defense of soft targets (schools, hospitals, sports facilities, etc.) has been identified as one of the priority activities. It should be noted that counter-terrorism is, as a rule, significantly more expensive than terrorism. For example, the total cost of Al-Qaeda's operation on 9/11/2001 was between 300.000 and 500.000 $ (Bilandžić, 2019). An important policy implication of historical and sociological research concerns what Chaliand and Blin (2007) describe as the need to avoid terrorism while claiming to fight it. In the fight against terrorism (on the ground and online), the importance of building instruments to prevent radicalization and international cooperation were also emphasized. According to Bilandžić (2019) this is the result of empirical analyzes which indicate that a reactive approach in the fight against terrorism is inappropriate and that a proactive approach is necessary to eliminate terrorism. To this end, mainly western countries, are working on the process of deradicalization (deterrence and social reintegration of radicalized individuals) and counter-radicalization (social and cultural contextual prevention of radicalization), which implies targeting the causes of terrorism, which has long been neglected in scientific research and policy actions against terrorism.

## 1.3 Intelligence

The term intelligence in English (in the field of security-intelligence terminology) describes several different terms: the name of organizations and systems that deal with the collection and processing of data and information; final written report provided to users of intelligence; but also, as the name of a (simplified) cycle/process, from planning and collection to processing and delivery of intelligence work (Leško, 2019). Although the generally accepted generic definition of intelligence in academia is not consistent, Kirkpatrick (1997) explains it by foreknowledge, which allows an appropriate response to external threats and protection of one's own interests. Intelligence contains an action element or a basis for decision-making and therefore has a qualitatively higher value than information (Herring, 2005). The central concept of the security-intelligence studies is the intelligence cycle. In a broader sense, the intelligence cycle is the transformation of information into intelligence (intelligence product). It originated on the division of military sciences and psychology (Phythian, 2014), and was first mentioned in 1948 in the book *Intelligence is for Commanders* (Glass and Davidson, 1948).

## 1.4 Project management

For the successful implementation of projects of various types, especially complex and more expensive projects, quality project management is necessary. According to Caspe (1976) project management is the art of coordinating resources and directing unidisciplinary groups so that the components of work performed by each group accumulates into a multidisciplinary team effort which achieves the desired objectives (or contracted scope of work) on time and within budget. In other words, it is a project, temporary endeavour undertaken to create a unique product or service (PMI, 2000). If an event planning process is to encompass both short-term requirements for the implementation of the event and the long-term objectives that become the legacies of the event, a model consisting of up to ten different stages is proposed (Masterman, 2004). Stages include defining objectives, concept, feasibility studies, decision to proceed, enter bid procedure (if required), implement planning, implement event, handover, evaluate and feedback. It is important to emphasize a key dimension of a project: project life cycle (initiation; planning; execution; performance and monitoring; closing). Both resources and costs vary at different phases of the project, increasing all the way through the execution phase when they reach their peak. As an example of mass sporting event, a drastic increase in costs over time (figure 1), makes sustainability one of the crucial challenges of hosting the Olympic Games.

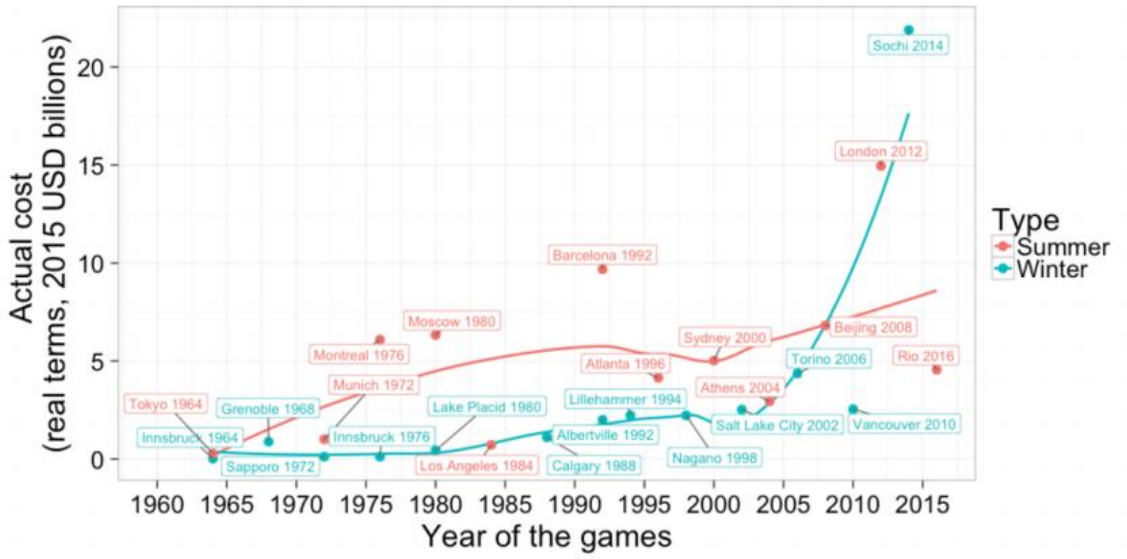


*Figure 1: Time series of costs for Olympics 1960-2016 (World Economic Forum, 2016)*

In terms of staff, the graph below illustrates an example of the rapid growth of paid staff for the London Olympics 2012, during the project life cycles.

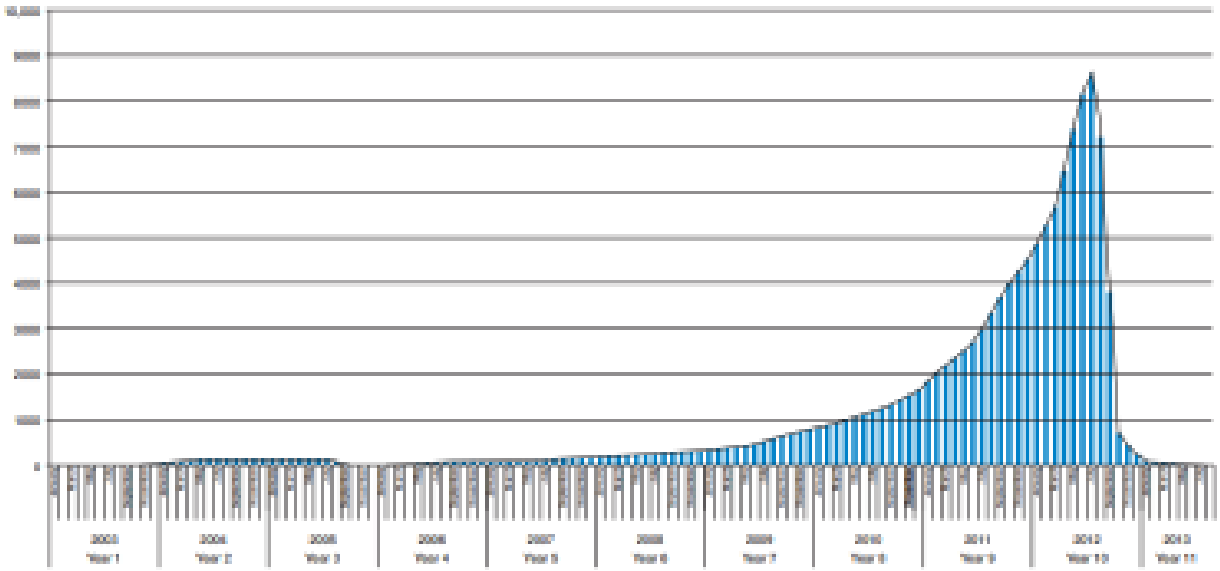

*Figure 2: The rapid growth of paid staff for the London Olympics 2012, during the project life cycles (IOC, 2015)*

Due to cost management and optimization, i.e., overall project success, the good governance is crucial. Governance is the act or process of governing or overseeing the control and direction of something (Merriam-Webster, 2022). Project governance provides direction and defines decision-making procedures and metrics for validating impacts to the project. It also enables the project team to deliver on requirements and creates a forum for issue resolution to occur in a timely manner (Alie, 2015). The figure 3 presents different phases of Project management.


*Figure 3: Phases of Project Management (Smartsheet, 2022)*

## 1.5 Security and safety in the project management of major sporting events

Sport is one of the most current phenomena of our era. From a special position since ancient times, from historical to Cold War competitions, boycotts of major sporting events and the use of sport as a geopolitical weapon, sport is gaining great attention in the political and security framework, especially nowadays. National sporting performance become an integral factor in the International Soft Power Index (Portland's in-house Content & Brand Team, 2018), and sport is also believed to influence global perception of countries (The Anholt-GfK Roper Nation Brands Index, 2009). At the United Nations level, sport is recognized as an instrument for contributing to sustainable development, peacekeeping and international communication (United Nations, 2005). 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). The concept of sport is associated with activities within sports clubs, and includes activities carried out during training and/or competitions organized by sports organizations (World Health Organization, 2006). Sport is a competition or activity which involves physical activity and skill, and takes place according to rules, for pleasure and/or as a job (Cambridge Dictionary, 2019). Various classifications of sport events can be made (Getz, 1997; Jago and Shaw, 1998; Boyer et al., 2007; Greenwell et al., 2014) and having in mind the complexity of staging a sport event and its possible impacts, different aspects of sport

events have been studied. The focus of this research is on top-level sporting events, which attracts the most attention of the global public. Quite a number of researchers studied success determinants at major sport events, mainly Olympic Games (more in Čustonja and Škorić, 2011; De Bosscher, 2016), sport event impacts and legacy (Bartoluci and Škorić, 2008; Preuss, 2015; Rogerson, 2016), etc. However, less attention has been paid to examining the providers, i.e., organizers' point of view (Škorić et al., 2017).

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), drawing additional attention to the importance of researching security and public space management during major sporting events and the social impact of such measures. A key question is how the securitization can be balanced with democratic principles and respect for human rights and civil liberties (Spaaij, 2016).

Terrorist attacks on events with mass gatherings can also be observed from the point of the so-called eventalisation, which assumes that incidents take on historical significance, as events that disrupt and destabilize previous ways of understanding the world (Foucault,

1991). 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. After 9/11/2001 sport entered a special focus of the US national security, where individual state security services became regular stakeholders in the conduct of sporting events (King, 2016). 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). In 2011, the European Union adopted a set of security measures for mass sporting events, with special emphasis on international cooperation in the prevention of terrorist attacks. Also, one of the initiatives was from the Council of Europe (2019), whose member countries have established a Committee for Safety and Security at Sporting Events.

The summer Olympic Games[2] are the leading international multi-sporting events. Their umbrella body is the International Olympic Committee, non-governmental sports organization based in Lausanne, Switzerland. The methodology of the Project Management Institute is largely applicable in the project management of the Olympic Games, within the methodologically based and transparent management is the main prerequisite for their successful implementation. In terms of project life cycles among the Olympics in general,

[2] In this thesis the research term Olympic Games also includes Paralympic Games, for all six case studies.

that timeline includes: initiation and bidding process; planning; execution; monitoring and controlling; closing.

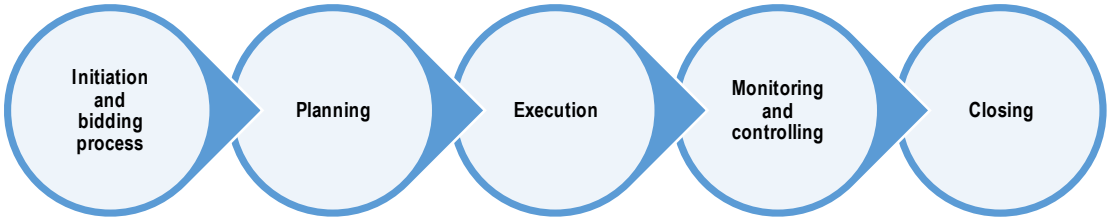


*Figure 4: Project life cycles among the Olympics*

At a core of the process of staging a (sporting) event is the organizing committee. It is a social entity as it can employ thousands of workforce members (paid staff members, volunteers, secondees, contractors) over the course of its existence (Parent, 2015) which can affect personnel management in both positive and negative way. In that sense, it is of crucial importance to have in mind several specific aspects for running a mega event: workers must be hired, trained and terminated within a relatively short time period, while these organizations tend to grow rapidly and may need to restructure several times during their life cycle (Xing and Chalip, 2012). Therefore, having experienced staff, especially when managing large-scale events, might be crucial to the point that the ability to organize the event is seen as one of the factors influencing successful candidature for hosting an event (Westerbeek et al., 2002).

The IOC Candidature Acceptance Working Group (2008) consider the summer Olympic Games require one of the largest security operations in the world and describe it as follows. Preparation takes many years of planning and the installation and absorption of new technologies can be complex. Training and rehearsing operational plans and procedures are time-consuming. Security agencies must be capable of absorbing this level of activity. In the context of the Olympic Games, the security operation includes the emergency services of the city/region/country that would respond to any critical incident threatening the safety or security of the population generally, including any person attending the Olympic Games. Safety and security also include the management of critical incidents, civil disasters or other events that threaten the safety of the population and the consequence management arrangements and capabilities in place. The human resources required for the security operation are very large and the personnel normally has to be deployed over an extended period of time, which could last for 50 days, 24 hours per day (from the date of the first "lock down" to the end of the Paralympic Games). Deployment on this scale has a significant impact on the city's ability to provide normal, everyday law enforcement to the community. The whole operation places the security forces of any country under considerable strain. The ability to withstand this pressure, respond to identified risks and prepare for critical incidents and their consequences over an extended time frame and theatre of operations, is an important requirement for Olympic Games security. The Olympic security operation assessment is based upon the potential performance of the security agencies proposed by the Applicant Cities. This is assessed for both the planning and operations periods of the Olympic Games. Previous experience of

the security forces in planning for and managing security operations for large scale sports and other events and the challenges that such environments present, are also taken into consideration. In the challenging and uncertain world security environment, many countries have invested in training and equipment for security forces to combat the threat and incidence of terrorism. This development has been taken into account in the overall grading of the assessment. The assessment is based upon information provided in the Application Files, as well as background security reports.

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 (OCOG). The host country authorities should work closely with the host city, OCOG and National Olympic Committee (NOC) to provide all the required services, including all financial, planning and operational aspects, to ensure the safety and security of all those involved in 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 OCOG, the home affairs ministry, the ministry of defense, intelligence agencies, cyber-

security agencies, the police and immigration and/or customs agencies. The multi-agency strategy should define the specific roles and responsibilities of each of the security stakeholders. The usual split of responsibilities is that the OCOG takes responsibility for security inside the venue perimeter, whereas the police or other agencies take responsibility for security outside the venue perimeter. Whilst delivering safe and secure Olympic Games, it is important to minimize disruption to the normal running of the host city's police service and other security services. When planning the security of the Olympic Games, it is important that the entire supply chain of goods is screened and remains protected, and close integration with the logistics department is required to achieve this (IOC, 2015). 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 date confirms that claim (more in the literature review chapter). 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 IOC 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).

Peter Ryan, one of the most experienced IOC experts, has expressed the view that it's probably just a matter of time before the Games are struck by a serious terrorist attack (Houston Chronicle, 2007). Each Olympics is larger and more complex than its predecessors. Traditionally, security at the Olympic Games was predominantly a domestic issue, it was managed by a variety of domestic agencies of the host country, best demonstrated by the efforts at the 1984 Los Angeles Games (Lawson, 1985). Both the Olympics and homeland security require coordination among all public safety disciplines, all levels of government, and the private sector. Both types of security operations require an effective way to share information that is timely, accurate, usable and secure (Oquirrh Institute, 2003). Security risks can never be completely eliminated and therefore must be managed (Oquirrh Institute, 2003). The resultant security measures aimed to protect the values of the Olympic Movement through the pre-identification of sources of threats that have effective means to threaten those said values (Krieger, 2019). The figure 5 presents the general risk management cycle.


*Figure 5: Risk Management Cycle (Counter Terrorism Protective Security Advice for Stadia and Arenas. NaCTSO, 2014)*

Over the recent period, the security and safety of the Olympics is no less extensive than for the events like The World Expo of G8 Summit. In that context, surveillance remains necessary. There is no doubt that surveillance and security are and should remain discrete concepts (Lyon and Murakami Wood, 2012), surveillance is an essential method of maintaining security at sports mega events. Security and surveillance practices at major sporting events have attracted considerable attention leading up to the London 2012 Olympic Games (Whelan, 2014). Lyon and Murakami Wood (2012) focus on distinguishing between security and surveillance by tracing the origins of security studies, as a sub-discipline of international relations, and surveillance studies, as essentially a multi-disciplinary field of inquiry centered on the practices of surveillance. They illustrate how these fields overlap in theory and in practice, but argue that security and surveillance need to remain distinct concepts. Security "speaks of a goal, an intended outcome, whereas

surveillance speaks much more of a practice, method, or means" (Lyon and Murakami Wood, 2012).

Considering a complex Olympic-related threats matrix, including terrorism, cyberterrorism, environmental/construction accidents, natural hazards, domestic crime, etc., Lechner (2014) pointed out who can be endangered:

1) Games Family (NOCs including their representatives, athletes, officials and staff as well as their equipment, personal belongings and public image; IOC including their members and staff as well as the Olympic brand; IFs including their representatives, officials and staff as well as their equipment and their public image; Partners/Sponsors including their staff as well as their brands; Broadcasters including their journalists and staff as well as their equipment; Athletes not belonging to an NOC (marching under the Olympic Flag) as well as their equipment and personal belongings; OC including their members and representatives as well as their public image)
2) Organizing Committee (OC members as well as their public image; Rented and own stadia, cars, offices, equipment, etc.; Employees, Volunteers and contracted or seconded workers as well as their personal belongings; Public image; Financial medium)
3) Spectators (within the stadia as well as other gatherings like public viewings, team houses and around the Games)
4) Host City/Host Country (Citizens, politicians and representatives as well as their personal belongings and buildings, offices and homes); International image and

reputation; Financial medium including influence on trade, tourism and currency; Public buildings, infrastructure and facilities.

# CHAPTER II:
# REVIEW OF LITERATURE

The literature review is divided into two parts. The first part includes security incidents at major sporting events in order to provide the necessary empirical background. The second part covers governance, work scope and budget for security and safety within the Olympic Games.

## 2.1 Security incidents at major sporting events

In a review of the Olympic security operations during the period 1972-1994, Sanan (1996) mentioned that those operations not only occur in a democratic context, but they also cannot spoil the joyous festival atmosphere, which is so special to the Olympic Games. He notes that the Olympic security should be both comprehensive and unobtrusive. Empirical data in the context of the Olympic Games, but also of sports in general, indicate tragic events and security incidents, as well as a number of prevented cases. Some of the highlights, such as the Munich Massacre at the 1972 Olympics or the concept of security in the Montreal Games four years later, have significantly influenced the change in security paradigms.

Ten days before the 1968 Ciudad de Mexico Olympics, tens of thousands of people, mostly students, took to the streets to protest the spending of public money on organizing the OG. They shouted out loud: “We do not want the Olympic Games, we want a revolution!” The government's response was brutal. The army carried out a massacre on

the Plaza de las Tres Culturas that lasted for about two hours (so-called Tlatelolco massacre). Although official estimates of the number of casualties have varied significantly, it is estimated that about 300 people were killed and thousands wounded (NPR, 2008; Sugden, 2012). The massacre during the 1972 Munich Olympics is certainly the best known when it comes to major sporting events, but also to historical terrorist attacks in general. Eleven members of the Palestinian terrorist organization Black September dressed in sports equipment, killed eleven members of the Israeli Olympic delegation and a German police officer in the Olympic village, which significantly affected further policies of Israel, Palestine and Germany. The event, witnessed by nearly a billion people on TV, is considered the beginning of the modern era of terrorism. Terrorism then became a public problem and an object of expertise. It was a turning point in the establishment of liminal studies of terrorism (Stampnitzky, 2013). On the same day, Israeli Prime Minister Golda Meir ordered the Israeli secret service Mossad Merkazi le-Modiin ule-Tafkidim Meyuhadim to carry out a secret operation to liquidate all those involved in the organization and implementation of the Munich massacre (Cronin, 2009). Over the next twenty years, Mossad members liquidated two of the three Palestinians who survived

Munich and at least twelve other Palestinians believed to have been involved in planning the action.

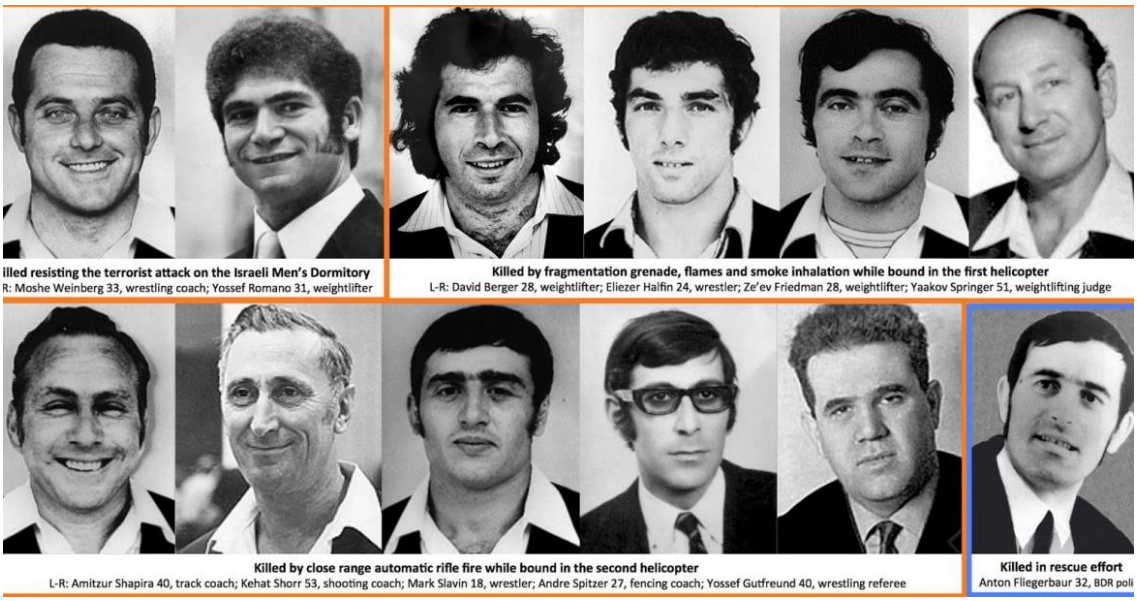


*Figure 6: Victims of the Munich massacre (Flickr, 2016)*

The tragic events in 1972 led the IOC to give the task to secure the Olympic Games to the Organizing Committees (Duckworth and Hunt, 2016). The turning point were the Olympic Games in Montreal in 1976, the first after the Munich massacre, considered to be the first Olympics with a visible security operation (Clément, 2017). Moreover, the Olympics are securitized. Securitization is a social process in which a question, phenomenon or problem is given security significance. It is an attempt to understand security through a socially and politically constructed process, through the discursive practice of social agents. When social agents talk about existential threats to benchmarks in order to win over the public (society) in terms of unacceptable violations of established norms and political practices and tolerating extraordinary measures that are not otherwise

acceptable, there is a case of securitization (Wæver, 2011). According to van Munster (2005), the structure of an act of securitization consists of three elements: a) the existential threat to the survival of an object; b) which requires special measures to be taken to protect and secure the object exposed to the threat; c) justifying and legitimizing "violations" of regular democratic decision-making procedures. According to Clément (2017) the Montreal Olympics, the largest sporting event in Canadian history, were also a turning point for the Canadian country. For the first time, terrorism took first place on the list of security threats, which until then had been reserved for communist subversions in Canada. According to security strategies, the Olympic Games in Montreal have been securitized, declared the target of threats that jeopardize the survival of the Games. Extraordinary measures have been taken to prevent threats and achieve security. The Montreal precedent became the standard for all later Games. Security strategy and security measures have transformed the Olympic environment into securitized and militarized areas, blurring the line between external and internal security, between civilian, police and military, and transforming the institutional design of the Canadian security system (Clément, 2017). In the official report, the Organizing Committee of the 1976 Montreal Olympic Games (1978) concluded that "Olympism survived" inside the Olympic village, implying that the increased security efforts did not have a negative impact on the athletes' experiences. Overall, the impact of terrorism on the Olympics has created a certain social legitimacy: their legacy goes far beyond the event itself, becoming the standard for the future. The Olympic Games have become one of the most important peacetime security events globally (Bilandžić and Leško, 2019).

In the years after the Montreal Olympics, terrorist activities have not disappeared. The Basque Euskadi Ta Askatasuna (ETA) claimed responsibility for an arson attack on a hotel close to the Olympic village two months ahead of the OG in Barcelona 1992 (Spaaij, 2016), and the leftist anti-fascist resistance group diverted Catalan gas pipeline the day before the Games. Activities led the security forces to no longer feel resigned to potential ETA disruptions during the Olympic Games (Riding, 1992). In total, the fears of domestic terror threats led to the deployment of 12 000 national policemen, 3 000 local police officers and an additional 10 000 military personnel for the 1992 Olympic Games. The official costs for security operations accumulated to approximately 210 million USD (IOC, 1992). Four years later, during the 1996 Atlanta Olympics, a bomb attack was carried out in the Centennial Olympic Park, killing one person and wounding 110 others. It was the first of four bombings perpetrated by Eric Robert Rudolph. Shortly after midnight, Rudolph placed an ALICE (field military package) under the bench that contained three bombs wrapped in 7.6-cm-long nails, which caused most of the injuries. Furthermore, one of the most important problems of the Sydney Olympics organizers in 2000 was the concern that the Games could become a terrorist target due to Australia's approval of US military interventions (Toohey and Taylor, 2012).

Exposure of major sporting events to threats in general and terrorism in particular, conditioned that security strategies and their implementation are an integral part of the organizational plans of such events, and additionally after the 9/11/2001. For example, experts called security measures at the 2006 Super Bowl "one of the largest security operations in American history", security at the Beijing Olympics in 2008 "the largest

peacetime security operation in Chinese history", and security at the London 2012 Olympics "one of the Britain's greatest security challenges since the World War II" (Bilandžić and Leško, 2019).

Furthermore in 2013, Dagestani Islamists carried out a suicide attack at the Volgograd railway station, as a threatening warning before the winter Olympics in Sochi, and Al-Qaeda in 2014 in its newspaper *Inspire* identified sports events as attractive targets, highlighting equestrian races, the US Open tennis and the English Football Premier League (Bilandžić and Leško, 2019). According to Lechner (2014), less than a month before the opening ceremony of the winter Olympics 2014 a militant group "The Helpers of Sunnah" claimed responsibility for the twin suicide bombings in Volgograd. The bombings killed 33 people and wounded 65 more. In their statement the group announced further attacks, targeting also the Sochi winter Olympics. It is supposed that this group is a subgroup of the Caucasus Emirate which aims to create an independent Islamic state in Russia's North Kavkaz (Soliyev, 2014). On the eve of the 2018 Football World Cup in the same country, a series of terrorist threats by the Islamic State emerged, calling on its supporters, the so-called lone-wolves, on attacks on that most popular football competition (Adelaide Now, 2018).

To acquire a broader picture, in a detailed analysis of terrorist attacks on sports facilities from 1970 to 2017, created using a Global Terrorism Database, Leško (2018) points to a drastic increase in the number of terrorist attacks that target sports. The figures 7 and 8 taken from that research clearly show an increase in the number of terrorist attacks

on sports facilities, but also a striking increase in the number of human victims of such attacks.

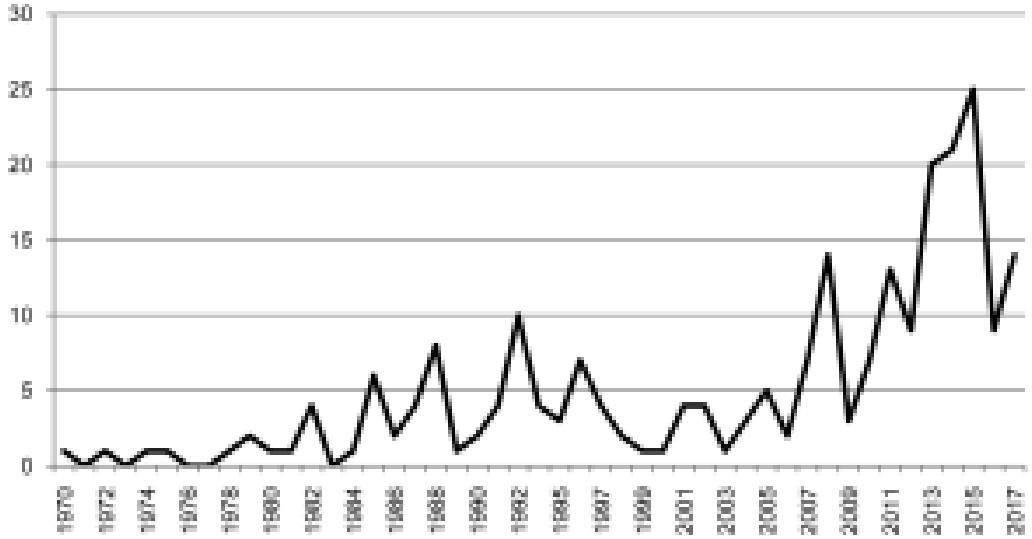


*Figure 7: Chronological overview of the number of terrorist attacks on sports facilities from 1970 to the end of 2017 (Leško, 2018)*

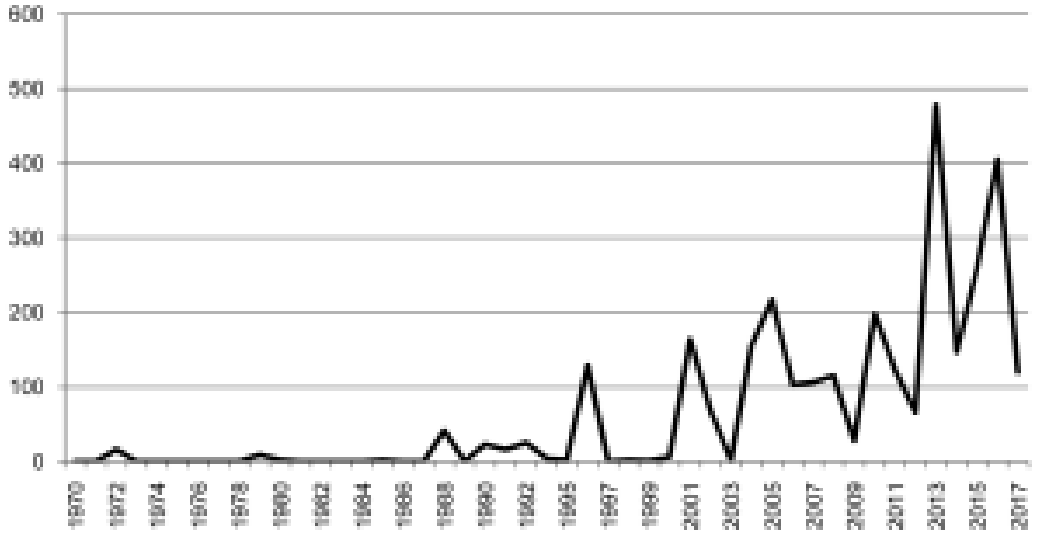


*Figure 8: Chronological overview of the number of victims of terrorist attacks on sports facilities from 1970 to the end of 2017 (Leško, 2018)*

In the same review article, Leško (2018) has analyzed different variables related to terrorism on sports facilities (table 1).

*Table 1: Different variables related to terrorism on sports facilities from 1970 to 2017 (according to Leško, 2018)*

| | |
|---|---|
| Number of terrorists attacks on sports facilities | 234 |
| Number of killed victims | 556 |
| Number of wounded victims | 2 490 |
| Average number of victims per attack (killed or wounded) | 13,01 |
| Number of countries in which terrorist attack on sports facility was carried out | 48 |
| Number of terrorists attacks on sports facilities with undetermined responsibility | 132 (56,41%) |
| Number of terrorists organization/group who carried out the attacks to sports facilities | 61 |
| Number of terrorists attacks to sports facilities towards readiness on dying | Non-suicidal (212) Suicidal (22) |

According to the presented data, Leško (2018) suggests that terrorism on sports facilities used to be more selective (discriminatory), while in a recent time its most common goal is mass killing of civilians (with property damage as collateral effect) in order to create psychological effect, i.e. to a collective fear and sense of insecurity prevailed. Analyzing

the number of terrorist attacks on sports facilities, Leško (2018) recorded the largest number in Asia (129), followed by Europe and Latin America, with 30 or more attacks each. Analyzing the number of victims of terrorist attacks on sports facilities by continent (killed or wounded), in the total observed period, most of them were recorded in Asia (1753), followed by Africa (471), Europe (402) and Anglo-America (386). Iraq (52), Pakistan (17), Afghanistan (12) and Colombia and Spain (10) are leading in the analysis of the countries with the highest number of terrorist attacks on sports facilities from 1970 to the end of 2017. In the total observed period, 61 terrorist organizations/groups were identified that carried out a terrorist attack on a sports facility or are suspected of doing so. Over time, some of these organizations ceased to operate due to their involvement in political processes, repressed by police/military/intelligence activities, or the terrorist organization achieved its goals. However, this statement does not stipulate that the newly formed factions will necessarily stop terrorizing (Leško, 2018). Associated with the highest number of attacks is ISIS (eight attacks), one of the most extreme and richest terrorist organizations in history (Weiss and Hassan, 2015), which initially originated as an Al-Qaeda franchise and defeated Iraqi security forces in June 2014 and declared a caliphate in parts of Iraq and Syria (a "state" entity in which Sharia law is applied under the leadership of a caliph, a religious and political leader). According to the specific location of the execution, Leško (2018) mentioned that most acts (76.06%) were committed in stadiums (internal or external perimeter), and the rest was committed in the internal or external perimeter of sports complexes, clubs, etc., with a slightly higher number of attacks on stadiums in 2000s (from 69.44% in the 1970s to 1999, to 79.01% in the 2000s). According

to the methodology of terrorist attacks in the world in general, the use of explosives is in the forefront, followed by firearms and incendiary devices. This order also applies to attacks on sports facilities (Leško, 2018). In the total observed period, the use of explosives prevailed (85.04% of cases), followed by armed attacks (8.11%) and the use of flammable substances (5.55%). Comparing with the results of Pizam and Smith (2000), who analyzed terrorist attacks on tourist destinations in the world from 1985 to 1998, and in which the largest number of attacks were carried out using firearms (45.30%), the results presented by Leško (2018) indicate that members of terrorist organizations in the context of attacks on sports facilities rationally choose explosive devices in order to increase the number of victims. According to the distribution of explosives, bombings dominated (77.38%), followed by the use of missiles and similar devices (12.56%). The use of bomb vehicles was recorded in 10.05% of cases. Explosives were placed in different ways. They were mostly detonated in columns when entering stadiums, during prevented entry into the control area and in the auditorium. There are cases when the funds are placed under the VIP sector, under the seats in the auditorium and in the locker room. Different forms of bombs were used, such as hidden time bombs or those left in briefcases, then remote-controlled bombs, sticky bombs, bombs hidden on the body or in the vehicle of a suicide bomber, etc. An explosive device was placed on the perpetrator's body in 17 suicide attacks while in 5 cases the suicide bomber's vehicle was loaded with explosives (Leško, 2018). The suicide bomber method is both "economical" and destructive, as indicated by the fact that, analyzing all suicide terrorist acts in the world in the period from 1982 to 2013, the

average number of deaths per suicide attack was 10.5, and the number wounded 28.4 (Bilandžić, 2014).

In order to identify empirical trends in terrorism at the Olympics especially, Spaaij (2016) has combined three major sources: the Global Terrorism Database, the National Security Archive's digital material, and the Cold War International History Project's digital archives. He counted twenty-two Olympic-related terrorist attacks from 1968 to 2014 (table 2) and concluded there is no consistent change in the frequency of Olympic-related terrorism over time.

*Table 2: Olympic-related terrorist attacks from 1968 to 2014 (according to Spaaij, 2016)*

| Year | Country | Fatalities | Description |
|---|---|---|---|
| 1968 | Mexico | Official death toll unknown; estimated at 100–300 | Ten days before the beginning of the 1968 Olympics in Mexico City, Mexican officials shoot and kill an unknown number of student and civilian protesters in Tlatelolco, Mexico City |
| 1972 | West Germany | 17 | Black September kidnaps and murders 11 Israeli Olympic team members (five athletes and six coaches) during the 1972 Munich Olympics. Five of the eight perpetrators and one West German police officer were also killed during the attack and subsequent hostage situation |
| 1976 | Barbados | 73 | Shortly after take-off a bomb explodes on Cubana flight 455 killing all 73 people aboard, including 24 members of the Cuban fencing team |
| 1983 | El Salvador | 1 | José Larios Guerra, former president of the Salvadoran Olympic Committee and retired Army Colonel, is assassinated by gunmen with suspected ties to the Farabundo Marti National Liberation Front |
| 1986 | Netherlands | 0 | 'Into the Blue Commando of the Revolutionary Cells' claims responsibility for bombing the headquarters of the 1992 candidature committee in Amsterdam in protest against Amsterdam's bid for the 1992 Olympics |
| 1987 | Israel | 0 | Tear gas assault on Jewish Olympic Games celebration |
| 1987 | South Korea | 115 | Korean Air flight 858 explodes in mid-air upon the detonation of a bomb planted by North Korean agents |
| 1992 | Spain | 0 | Euzkadi Ta Askatasuna (ETA) is suspected in an arson attack on a hotel near the Olympic village two months before the 1992 Barcelona Olympics |
| 1992 | Spain | 0 | The Grupo de Resistencia Antifascista Primo Octobre (GRAPO) bombs a gas pipeline in Catalonia the day before the opening ceremony of the 1992 Barcelona Olympics |
| 1996 | Colombia | 1 | A Russian Olympic cyclist is kidnapped and killed by the Revolutionary Armed Forces of Colombia (FARC). The cyclist was on a transcontinental bike tour towards the 1996 Atlanta Summer Games. His body was found a year later near the Panama border |
| 1996 | United States | 2 | Eric Rudolph bombs Atlanta's Centennial Park during the 1996 Atlanta Olympic Games, killing two and injuring more than 110 others |
| 1997 | Greece | 0 | The Greek Olympic Committee is bombed by members of the Anti-Authority Group |
| 2004 | Greece | 0 | A group using the names of the mascots of the 2000 Athens Olympics, Phevos and Athena, claims responsibility for fire-bombing two Environment Ministry trucks during IOC meetings in Athens |
| 2005 | Spain | 0 | ETA claims responsibility for a car bomb attack outside the Pieneta track and field complex used to promote Madrid's bid to host the 2012 Olympics. The attack comes less than two weeks before Madrid's bid to host the Games |
| 2006 | Iraq | 3 (at least) | The President of Iraq's Olympic Committee, Ahmed al-Hejea, its Secretary-General, Amr Abdel Jabbar, the head of Iraq's taekwondo federation, Jamal Abdel Karim, the head of water sports, Saeb al-Hakim, and dozens of other officials and athletes are abducted in a series of kidnappings between July and December 2006. An unspecified number of victims are killed or remain missing |
| 2008 | China | 0 | An improvised explosive device is found in Beijing's Qinhuangdao Stadium where the Olympic football matches are to be held |
| 2008 | China | 2 | A knife-wielding assailant murders an American businessman and injures his wife and their tour guide. Their son-in-law was the coach of the US men's volleyball team |
| 2008 | China | 3 | Two bombs explode on Chinese buses in Kunming, Yunnan province, less than three weeks before the Beijing Olympics. The Turkistan Islamic Party claims responsibility for the bombings but Chinese authorities reject this claim |

(*Continued*)

| Year | Country | Fatalities | Description |
|---|---|---|---|
| 2011 | Pakistan | 1 | Unknown gunmen kill Absar Hussain, three-time Olympic boxer and Deputy Director of the Pakistan Sports Board, as he leaves the Ayub Stadium in Quetta |
| 2012 | Libya | 0 | Assailants kidnap the President of Libya's Olympic Committee, Nabil al-Alam, in Tripoli. He is later released |
| 2013 | Russia | 19 | A suicide bomber detonates at a train station in Volgograd. Vilayat Dagestan claims responsibility for the attack, framing it as a warning ahead of the 2014 Sochi Winter Olympics |
| 2013 | Russia | 17 | A suicide bomber detonates on a trolley bus in Volgograd. Vilayat Dagestan claims responsibility for the attack. |

Fears resulted in the IOC 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). Due to all the above, as well as the complication of security threats in modern conditions, security in general and (counter-terrorism) are particularly central points of organizing major sporting events (Giulianotti and Klauser, 2012, Bilandžić and Leško, 2019). Also, in recent years, various negative referenda have resulted in cancellations of Olympic bids. In Germany, local citizens have rejected two bids, for the 2022 winter Olympic Games in Munich and the 2024 summer Olympic Games in Hamburg. An omnipresent argument by those campaigning against the Olympics was that of high costs, caused mainly by rising security budgets. The resultant security measures aimed to protect the values of the Olympic Movement through the pre-identification of sources of threats that have effective means to threaten those said values (Krieger, 2019).

Countries hosting major sporting events are also facing forms of cyber-attacks. It has been reported that the Beijing Olympics in 2008 suffered about 12 million cyber-attacks during each day of their duration (Ormsby, 2010), but it is not known whether (and how many) of these attacks were terrorist-motivated. Cyber threats come from individual attackers (crackers), from hacktivists, from cybercriminals and those driven by the support of national systems that have the best resources at their disposal (Advanced Persistent Threats). In that order, it is useful to explain some basic cyber-crime related terms:

- (Spear) Phishing: An attacker sends a fake message designed to deceive a human victim in order for that person to reveal sensitive information to the attacker or for the attacker to upload malicious software to the victim's digital infrastructure.
- Whaling: Targeted attack by cybercriminals on prominent individuals, with the aim of stealing money or sensitive information or gaining access to their computer systems for criminal purposes.
- Vishing: Criminals contact a potential victim over the phone pretending to be a company/organization and trying to persuade them to share personal information.
- A distributed denial-of-service (DDoS) attack: A malicious attempt to disrupt the traffic of a targeted server, service or network by overwhelming the target or its surrounding digital infrastructure with a flood of internet traffic.
- Malware (computer spyware, viruses, computer worms, trojans and bots): Programs that can capture everything typed on someone's computer, take screenshots, steal documents, etc. This information is sent to the person who installed the malware.

- Ransomware: A form of malware designed to encrypt files on a device, making all files and systems unusable. Malicious actors seek ransom in exchange for decryption.

The Montreal-based World Anti-Doping Agency (WADA) has encountered an attempt by Russian hackers to break into a computer system (The Star, 2017). It is believed that the retaliatory attacks for the discoveries just before the 2016 Rio de Janeiro Olympics about the widespread doping of Russian athletes in dozens of sports sponsored by the Russian country were corroborated by testimonies from Russian whistleblowers. After the International Olympic Committee, with certain exceptions, allowed Russians to participate in the Rio de Janeiro Olympics, anti-doping agencies issued a joint statement expressing deep opposition to their performance. Then the cyber-attacks began. The Fancy Bear group (also known as APT-28) has announced that it has broken into a system containing controversial medical records of thousands of athletes, including famous names like Rafael Nadal Parera and Serena Jameka Williams (Tennismash, 2016). Experts believe that Fancy Bear works closely with the Russian Military Intelligence Service/Glavnoye razvedyvatel'noye upravleniye or GRU (MIT Technology Review, 2019).

Since the security budget of major sporting events has increased exponentially, the data indicate a lower number of attacks, i.e. effectiveness in preventing terrorist attacks at major sporting events, which resulted in a change in targets of attacks on less exposed but also massive sporting events, especially in the Middle East (Leško, 2018). Considering the statement that the threat posed by terrorism to the western world is less based on facts and

more on imagining the worst-case scenarios (Šušnjara, 2017), as well as data indicating fewer attacks on western sports facilities in the 2000s, it is noted that in the western world (Angloamerica and Europe) terrorism on major sporting events is not a high probability that will happen. Terrorist attacks on the Olympic Games were recorded predominantly in the last century, in 1972, 1992 and 1996. Although it was concluded in 2006 that major sporting events (especially the summer Olympics) were the most frequent targets of terrorist attacks (Horne and Manzenreiter, 2006), cyberterrorism seems to be a more frequent threat to the contemporary Olympics. This is partly due to the drastic increase of investment in counter measures against terrorist attacks, and partly due to the current potential of cyberterrorism, which can cause great damage without the necessary physical presence of terrorists (Bilandžić and Leško, 2019). It is important to point out that, despite numerous recorded attacks, terrorism has failed to significantly hamper the holding of major sporting events (Hassan, 2012), which remains true nowadays given the continuous holding of the summer and winter Olympics.

## 2.2 Governance, work scope and budget for security and safety within the Olympic Games

The generation of post-9/11 uncertainties has escalated the scope of Olympic security, which extend contemporary developments in global security governance in general. 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). Due to cost management and optimization, i.e., overall project success, the good governance in the domain of security and safety among the Olympic Games is crucial. According to Oquirrh Institute (2003), all Olympic incidents were local incidents first. All homeland security incidents also affect local communities first. Securing the homeland starts from the bottom up. This means local efforts are an integral part of any national security effort. However, broader processes of transnational and multi-agency collaboration and knowledge transfer are also centrally implicated in this process (Spaaij, 2016). Zekulin (2009) has demonstrated that planning Olympic security is a formidable task in part due to three challenges: logistical issues, interagency cooperation and a reliance on volunteers. 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). The more parties involved, the more difficult it is to attain consensus on the best way forward. 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. The reality is that different people, or in this case, 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 (Oquirrh Institute, 2003).

In the other hand, jurisdictional issues lead to hierarchy and power-sharing disputes at even at the most basic level of security planning. One such example was observed during the lead-up to the 1996 Summer Games in Atlanta. In one of the final meetings prior to the opening of the Games, Vice President Al Gore interrupted the FBI presenter with one simple question: "Who is in charge?". When no one voiced an answer, he once again posed the question and was told that "it all depends on the situation" with no further elaboration offered (Suburban Emergency Management Project, 2005). The Atlanta problems were so serious that an emergency re-organization of the entire Security Support Group tasked with planning the Games occurred mere months prior to the Games began (Boyle and Haggerty, 2009). Publicly, a united front is always projected, but behind the scenes, in-fighting, mistrust and "organizational inferiority complexes" exist (Bellavita, 2007). The 2002 Salt Lake City Games involved more than 100 local, state and federal agencies and a study following the Games revealed numerous problems among the various agencies (Oquirrh Institute, 2003; Zekulin, 2009): "Firefighters were seen as lazy. Public work was fragmented. Private and corporate security personnel were viewed as rent-a-cops. Emergency medical groups were looking for someone to tell them what to do. Public health agencies only seemed able to hold meetings. Infrastructure owners did not want to tell anyone about their vulnerabilities. Everyone was afraid the cops would get more than any

other group. The National Guard and the active-duty military component disagreed about almost everything; the Secret Service was reluctant to share anything. The FBI worried another agency would invade its turf. FEMA was fretful it would not get called to meetings and the US Attorney kept sticking his nose into everyone's business. Federal law enforcement agents brought in to help plan the Games looked at Utah public safety as a collection of well-meaning but naïve hicks. In turn federal agents were seen as arrogant and inept Rural agencies didn't trust their urban counterparts. Sheriffs didn't trust police. Neither trusted the State. No one trusted Washington. And Washington returned the favor." This illustrative example unequivocally confirms the importance of governance within the security and safety processes among the Olympic Games, both preparation and execution. Oquirrh Institute (2003) summarized some governance-related lessons learned from the security preparations and execution at the Salt Lake City 2002 winter Olympics: blend central coordination with local control; build an institutional framework; build social capital; rely on networks, not on a mainframe; integrate homeland security into all public safety activity.

The scope of security and safety work among the Olympics is quite complex, while risk analyses change depending on the location of the Games. For example, one determining factor is the geophysical and geopolitical location of the country which is hosting the Games (Oquirrh Institute, 2003). Also, large numbers of attendees allow individuals to "blend in" with crowds making it difficult to identify them. Proximity of events to transportation hubs allows for quick and easy escape, and event-associated hospitality sectors (hotels, restaurants, etc.) also have a potential to be affected, thus

"increasing the scope of the reach and impact of any terrorist incident" (Toohey and Taylor, 2008). According to Krieger (2019) the brief summaries of the security operations at the respective Summer Olympic Games in the 21st century demonstrate that 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. Hence, the security costs exploded following the terror attacks in the United States, the United Kingdom and Spain in the 2000s. That said, it is equally important to consider the socio-political environments of host cities when discussing Olympic Games security operations. 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. Another issue is relation between major sporting events and mass media. According to Tulloch (2000), the mass mediation and political framing of the terrorism-Olympics nexus have become embedded in people's routine daily knowledge, experiences and anxieties by preparing people for the possibility of terrorism and by normalizing the extraordinary measures designed to combat it. Horne and Manzenreiter (2006) have predicted that security issues are likely to come more to the fore in production of sports mega-events and will form a substantial research theme in further studies of major sporting events. Despite mentioned, Spaaij (2016) mentioned that terrorism and security have received less academic scrutiny than other aspects of the Games, but in recent years, research on

terrorism and security at the Olympics and other major sports events record certain increase. Contributions to the knowledge have come from a range of fields including history, sociology, criminology, political science, international relations, sport management, etc. It is timely to take stock of these contributions and identify how they inform, or can inform, intellectual and public understandings of terrorism and security at the Olympics (Spaaij, 2016). Furthermore, in a scientific book that conceptually considers the relationship between sport and national security, Bilandžić and Leško (2019) propose a framework that generates at least three reasons for including sport in security studies in general and terrorism studies in particular, in the context of sport and national security. and the negative (internal and external) effects of sport on relevant elements of national security. These are: Sport and national identity (national cohesion); Sport, international reputation of the state and sports diplomacy; Sport as a target and instrument of security threats.

Theoretical, empirical and analytical evidence suggests that sport, sporting events and their actors have security dimensions and are in a causal and correlated relationship with security, which is why sport should be part of security studies. Such conclusions are empirically confirmed in key documents of the highest rank, national security strategies. Such strategies are a national guide to achieving national security (Bilandžić and Leško, 2019).

Considering the security of sports facilities, experts warn that the lack of training of security staff on stadiums is one of the main risks to terrorism (Baker et al., 2007;

Cunningham, 2007), and Hall (2006) summarizes eleven important categories of security activities on sports facilities:

1) Control of the perimeter of the sports facility;
2) Access control to the sports facility;
3) Supervision of the accreditation system;
4) Physical protection systems;
5) Risk management;
6) Emergency management;
7) Recovery procedures;
8) Communication systems;
9) Security staff;
10) Training (modeling and simulations);
11) Protection from toxic materials and weapons of mass destruction.

According to Leško (2018), empirical data also point to the importance of quality security and safety preparation, which includes: integrated risk (and vulnerability) assessment; empirical and analytical implementation of security audit in sports facilities and their accompanying premises and facilities; analysis of measures of mechanical, technical and physical protection of the external and internal perimeter of the sports facility, as well as control of the airspace over the sports facility due to the potential drone threat; use of quality technology to detect the introduction of potentially threatening objects into sports facilities; etc.

Considering security risks among the Olympics, Giulianotti and Klauser (2010) place them in three categories: a) terrorism; b) spectator and political violence; c) poverty, social divisions and urban crime. Terrorism has been a key risk for every Olympic Games since the 1972 Munich Games regardless of the threat environment experienced in the host city (Giulianotti and Klauser, 2010; Jennings, 2012). According to the IOC Candidature Acceptance Working Group (2008) the following sub-criteria were taken into consideration:

a) The incidence and likelihood of terrorism;
b) The levels of known recorded crime and other public safety issues;
c) The overall technical and professional competencies of the main security forces and the proposed command and control;
d) The existing investment in security and related technology and the proposals to improve in this area to meet the Olympic Games security requirements;
e) The complexity of the proposed Olympic Games "theatre of operations" and the required security response.

The theatre of operations refers to the entire Olympic Games geographic area of activities and all of the villages, venues, facilities, transportation systems and public places used to support the Olympic Games. The number of resources, logistic and technical support, adequately trained personnel and their deployment are all affected by the complexity of the overall proposals, including the geographical spread of venues and facilities, the terrain and the transport network. Thus, the overall complexity of a security

planning and operational response for the proposed Olympic Games theatre of operations is given due consideration in the assessment and weighted accordingly (IOC Candidature Acceptance Working Group, 2008). In carrying out an assessment of the risk of terrorism in the Applicant Cities, the Working Group concluded that any city in the world can be subject to a terrorist attack either by local or international terrorist groups. However, some Applicant Cities were considered to be more at risk due to the current uncertain security situation and the threat levels in neighboring countries in the region which could impact the Olympic Games. The ability of cities to deal with and manage this risk was taken into account. Nevertheless, the Working Group was sensitive to the difficulty of trying to assess the security situation eight years before the 2016 Olympic Games. However, the risk to Candidate Cities will need to be continuously monitored to take into account changing world circumstances (IOC Candidature Acceptance Working Group, 2008). The Working Group also took into account the fact that proposals for security operations in the build-up to and during the Olympic Games can be amended more easily to meet the assessed threat than, for example, the provision of fixed Olympic Games infrastructure. It would not be appropriate in a public document to detail all the issues of security raised and considered by the Working Group. However, some comments can be made.

A significant number of resources is devoted to intelligence and surveillance activities targeting potential security risks in the lead up to any sports mega event. This was made clear in the security strategy for London 2012 (Home Office, 2011a, 2011b). While virtually all analysts recognize that "sporting mega-events involve a level of organization unmatched outside of wartime and planning that requires significant

alterations to the governance of the host city or country" very few have sought to examine how security agencies and agents, which in the case of London 2012 numbered in excess of 40 000, are organized (Fussey and Coaffee, 2012a). It is also acknowledged that, when security problems have occurred at mega sporting events, it is the coordination and communication components that have proved to be both crucial yet are also the most common points of failure (Fussey and Coaffee, 2012a). While bringing attention to the issues of communication and institutional structures, and the ways in which event organizers have attempted to deal with these challenges, Boyle (2012) also makes the point that these are complex questions involving, inter alia, issues of expertise, culture and trust. These questions are fundamentally about 'networks' (Whelan, 2012). One of the challenges Olympics 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). At the 2012 London Olympics, there was constant monitoring and recording of spectators and locals via cameras and CCTV, helicopters and drones, increased presence of military personnel, extensive MI5 preparations and the Department of Defense (King, 2016). As the facial recognition technology advances, the threats to privacy consequently increase. With biometric facial recognition, the loss of information privacy essentially takes two forms: fears of tracking and clandestine capture. Tracking refers to the ability to monitor an individual's actions in real time or over a period of time. In its most extreme incarnation, tracking could become a kind of "super surveillance" that lets the tracker "follow" a person today as well as search databases to learn where he was months ago (Woodward, 2001). According to Woodward (2001) biometric facial recognition can provide significant

benefits to society. Biometric facial recognition is by no means a perfect technology, and much technical work has to be done before it becomes a truly viable tool to counter terrorism and crime. But the technology is getting better and there is no denying its tremendous potential. In the meantime, we, as a society, have time to decide how we want to use this new technology. By implementing reasonable safeguards, we can harness its power to maximize its benefits while minimizing the intrusion on individual privacy (Woodward, 2001).

The following are selected components that the Oquirrh Institute (2003) have identified as an example of good practice within the security and safety of the 2002 Winter Olympics in Salt Lake City, the first Olympics after the 9/11 attacks. The Utah Olympic Public Safety Command (UOPSC) model was established in order of protecting the Games from undetermined risks; developing and implementation of a plan that used resources responsibly to protect the Games and the communities in Utah; maintaining an environment consistent with the spirit of the Games and the image of the United States. Regarding the institutional framework The UOPSC model was created in state statute and clearly defines its membership, duties, and powers. It provided a laboratory to explore a variety of command, control and coordination mechanisms. The command became an effective coordinating group because it included representatives from state, local and federal agencies and from the private sector. They subdivided planning into 12 individual programs: research; design; master plan; plan management; subcommittee plans; resource identification and acquisition; training and testing; transition; operations; Paralympics; recovery; after action. Also, they have organized Functional Working Groups, coordinated

by full-time planners and were comprised of representatives from agencies responsible for managing or supporting each function. These groups included: human resources, accreditation, international entry, communications, research, intelligence, infrastructure protection, dignitary protection, federal affairs, military affairs, aviation, fire and emergency medical services, explosive ordnance disposal, venues and village security, private security, traffic, protocol, emergency management, community and media relations, etc. Regarding the venue security, they emphasized commit to quality and cooperation; including possible terrorism in plan; early coordination between state and federal agencies; use progressive planning and training; locate dispatch personnel on-site; log and track equipment; screen vehicles; use closed-circuit television closed-circuit television; use civilian volunteers. In terms of federal involvement, they emphasized Interagency Cooperation; Conduct In-depth Reviews of Future Bids; Conduct In-depth Reviews of Future Security Plans; Recommend a Federal Central Coordinating Office. Regarding the military involvement (the National Guard and the DOD The military provided over 3 500 people to help secure the Games), the military was responsible for or supported the venue sweep; perimeter posts; vehicle screening areas; operations; all pedestrian entry points. They have also established policies for law enforcement volunteers, but also for the fire, emergency management services and public works and emergency management. A special attention was paid into recruiting and building personal and working relationships as well as training (overview of Olympic operations, specialty training, field exercises, venue-specific training, product/equipment training). Over 3 000 (of UOPSC's 12 000) public safety officers received the basic UOPSC Olympic training.

Almost 60 scenario-based tabletop and field exercises were conducted. The next important segments were accreditation credentialing system and the incident tracking. for gathering and disseminating sensitive information, the UOPSC used a proprietary computer system, called "E-Team". It was the primary means for incident reporting and distributing intelligence. The system was also used for information management, situation awareness, and resource management. Other critical elements were also incorporated in the system (infrastructure for hospitals, shelters, and transportation systems; availability of hospital beds and medical personnel on a daily basis; other real-time updates on capacity for emergency medical decision makers). More than 1 700 incident reports were created and modified. Primary incidents reported included suspicious persons and packages; transportation-related events; and bomb threats. The Oquirrh Institute (2003) emphasizes the importance of reliable communication systems, which is crucial for example in the Explosive ordnance disposal plan. Finally, the job of the Olympic Intelligence Center was to collect, evaluate, analyze, and disseminate relevant, accurate, and timely intelligence. More than 60 federal, local, state and international agencies participated in UOPSC's intelligence operation. The Olympic Intelligence Center was made up of three main components: 1) Counter-terrorism Intelligence Section formed by the FBI, 2) Critical Intelligence Collection, Analysis, and Dissemination Unit formed by the Utah Department of Public Safety and other state and local agencies, 3) Dignitary Protection Intelligence formed by the United States Secret Service. Similarly, Connors (2007) mentioned key functional areas within the security and safety among the major special events, which can be applicable also to the Olympic Games (figure 9).


*Figure 9: Major Special Event Security Key Functional Areas (Connors, 2007)*

Figure 10 presents security zones of major sporting events.

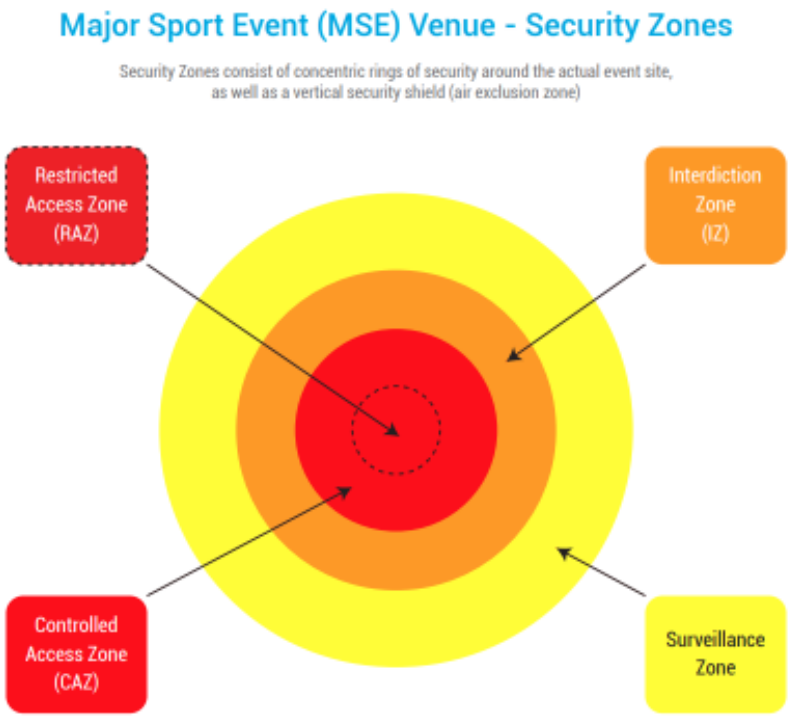


*Figure 10: Venue Security Layers (Zones). Explains the configuration of the concentric security rings recommended to protect MSE venues and, to a lesser extent, the non-venue sites located in the surrounding urban domain. In: United Nations Office of Counter-Terrorism (2021): Guide on the security of major sporting events*

With each new Olympic Games in recent times, cyber security is becoming an increasingly important component of the security work scope within the Games. This is also applicable to other major international sports competitions such as the World Cup in football. Khalifa (2020) aimed to identify cybersecurity threats expected at the upcoming FIFA World Cup in Qatar in 2022 and assess how they can be prevented. The results revealed high loadings of potential cyberattacks on sponsors, fans, online ticket sales, government and the FIFA website based on the PCA. The regression analysis revealed a statistically significant association between the perception of the cybersecurity risks and

perceived quality of measures undertaken to address the cyber threats. Crelier (2019) compared the cyber threats for G20 summits and the Olympics. He found that both types of events were impacted by similar cyber incidents. The distinction was that G20-related attacks were mostly connected with cyberespionage, and were less directed at destruction and damaging the image of these summits or hosting countries. Along with that, more detailed recommendations for protection from cyberattacks may include setting up systems of threat gathering before, during, and after events; control of information flows to elude intrusion into servers; testing security systems for potential vulnerabilities; training of employees regarding information security and ways of protecting from cyberattacks; compliance audits of contractors and third parties; and formulating a plan of actions for the case of attacks (TrendMicro, 2018). Among the most frequently used methods of attacks are phishing and Distributed Denial of Service (DDoS) attacks. Cases of both types of attacks were evidenced during all the latest major sporting events, including the Olympics of 2008, 2012 and 2016 and the World Cups 2014 and 2018 (Cooper et al., 2012; TrendMicro, 2018). Besides, an effective system of measures including discouragement of any financial operations through public networks, avoidance of using suspicious devices such as USB drives, full encryption of devices used by players and auxiliary staff and organizers, and appropriate cyber protection of infrastructure networks, allowing the country to host the tournament without cyber scandals (Goud, 2018).

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). Additionally, 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 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). As a result of

the 9/11 terrorist attacks in the USA, the 2002 winter Olympic Games developed into the largest domestic security operation ever undertaken in the United States (Decker et al., 2005). According to the Oquirrh Institute (2003), total security budget in the Salt Lake City winter Olympics 2002 was 310 million USD (272 million were direct federal expenditures, while state and local governments spent the remaining 38 million), much more than for summer Games in Atlanta 1996, where the federal government alone contributed 101 million to a total of around 200 million official safety and security-related projects (Krieger, 2019). Being the first major event after the 9/11/2001, the 2002 Winter Olympic Games quickly became the US's first homeland security effort. No significant security incidents occurred during the Games. This success coupled with our unique model provides us with an opportunity to share valuable information with others (Oquirrh Institute, 2003). When the City of Vancouver submitted its bid to host the 2010 Winter Olympic Games, the cost of providing security for the event was estimated at approximately 175 000 000 $, one-third of the final actual budget of 558 000 000$ (Plecas et al., 2010). Giulianotti and Klauser (2010) highlight this trend in relation to the increasing economic costs of security measures and numbers of personnel.

An additional challenge is the fact that in some countries that have hosted major sporting events, systematic social injustices have been witnessed, given that hundreds of thousands of citizens have been forcibly relocated from their homes (Sudworth, 2006). Because of that, but also because of investing in sports infrastructure at the expense of investing in essential infrastructure in terms of schools or hospitals, protests were witnessed, some of which ended tragically. In Brazil, there have been frequent protests

over the organization of the 2014 Football World Cup and the 2016 Olympics (Gaffney, 2016). Encouraged by the publicist effectiveness of the protests in Brazil, the protesters organized further strikes and public actions in 2013 and 2014 around the world. One of the federal government's responses was to create 10 000 military strike forces, which could be quickly deployed to potential protest locations during the World Cup if needed. These forces, combined with 1.9 billion Brazilian reals (about half a billion USD) in federal security spending and an additional 15 000 security officers, prevented and prevented protests for the duration of the tournament (Bilandžić and Leško, 2019).

Much of the literature focuses on three overlapping issues: a) security legacies of sports mega events (e.g., Bennett and Haggerty, 2011; Coaffee et al., 2011; Fussey et al., 2011; Fussey and Coaffee, 2012b); b) security risks and the infrastructures and technologies used in an attempt to manage those risks (Fussey and Coaffee, 2012a; Giulianotti and Klauser, 2012; Richards et al., 2011); and c) the overall "security spectacle" that characterizes sports mega events (Boyle and Haggerty, 2012). As terrorism and security have received less academic scrutiny than other aspects of the Games (Spaaij, 2016), this dissertation will complement previous research in terms of analysis and comparation of governance, work scope and budget within the last six summer Olympic (and Paralympic) Games. As a systematic review, this research will expand both theoretical and empirical knowledge in the field of security and safety among the contemporary Olympic Games, events that are without a doubt, one of the world's largest peacetime security challenges, and through which countries (and community) achieve long-term legacy in the form of infrastructural, technical and personnel security achievements.

# CHAPTER III:

# 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:

1) Security and safety of the Sydney 2000 Olympic Games
2) Security and safety of the Athens 2004 Olympic Games
3) Security and safety of the Beijing 2008 Olympic Games
4) Security and safety of the London 2012 Olympic Games

5) Security and safety of the Rio de Janeiro 2016 Olympic Games
6) Security and safety of the 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 3). 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 3: Case studies related sources*

| CASE STUDY | SOURCES |
|---|---|
| **Sydney 2000** | • ASIO. 2000. Report to Parliament 1999-2000.<br>• 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.<br>• 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.<br>• 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.<br>• 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. 2011a. London 2012 Olympic and Paralympic Safety and Security Strategy. UK Government, London.<br>• Houlihan, B., & Giulianotti, R. 2012. Politics and the London 2012 Olympics: the (in)security Games. International Affairs 88, 4, 701-717.<br>• House of Commons Home Affairs Committee Olympics Security Seventh Report of Session 2012-13.<br>• 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.<br>• Halchin, L.E. & Rollins, J.W. 2016. The 2016 Olympic Games: Health, Security, Environmental, and Doping Issues. Library of Congress. Congressional Research Service.<br>• 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.<br>• 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.<br>• 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.<br>• The Tokyo Organising Committee of the Olympic and Paralympic Games. 2021. Update to the Sustainability Pre-Games Report. |

Data analysis includes qualitative 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; qualitative 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; and quantitative 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. The limitation of this research is the fact that certain security data were classified as confidential and therefore exclusively open-source data was used.

# CHAPTER IV:

# RESULTS

## Introduction

The risk assessment changes depending on the location of the Olympic Games. For example, one determining factor is the geophysical and geopolitical location of the hosting country (Oquirrh Institute, 2003) while certain threats, such as terrorism, remain persistent. During mass gatherings it is more challenging to detect individuals with hidden intentions. Proximity of events to transportation hubs allows for quick and easy escape, and event-associated hospitality also have a potential to be affected, thus increasing the scope of the reach and impact of any terrorist incident (Toohey and Taylor, 2008). Therefore, security expenditure for every edition of the Olympic Games rise, where a significant amount is represented by taxpayers' funds. Adding the impact of securitization on the restriction of fundamental human liberties, as well as emphasized global publicity, it is important to research conceptual empirical approaches to the security and safety of such mass events. The following sections present six consecutive case studies on security and safety at the Olympic (and Paralympic) Games with a special focus on governance, work scope and budget:

1) Sydney (Australia) 2000;
2) Athens (Greece) 2004;
3) Beijing (China) 2008;
4) London (United Kingdom) 2012;

5) Rio de Janeiro (Brazil) 2016;

6) Tokyo (Japan) 2021.

## 4.1 CASE STUDY: SYDNEY 2000

Even though Australia was considered a low security threat, the Sydney Games, the first in the new millennium, witnessed the largest security operation in Australia's history (Toohey and Taylor, 2012). According to the Australian National Audit Office's Commonwealth Agencies' *Security Preparations for the Sydney 2000 Olympic Games Report* (1998) the Sydney Organising Committee (SOCOG), through the host city contract with the IOC and by agreement with the Sydney 2000 Paralympic Organising Committee, was responsible for the delivery of the security program for the Games. The Australian National Audit Office's Commonwealth Agencies' (1998) illustrates a security and safety governance: the SOCOG has contracted its government agency security planning requirements through the Olympic Security Working Committee (OSWC) to the New South Wales Police Service. In addition, the Commonwealth Government had constitutional responsibility for such aspects of security as border control, aviation security, dignitary protection, counter-terrorism planning and certain aspects of law enforcement. The OSWC has divided the security program into thirteen sub-programs, each with a work group responsible for planning with respect to their sub-program area (substantial representation by Commonwealth agencies among most of the workgroups). The NSW Police have established the Olympic Security Command Centre to coordinate and direct the workgroups and to manage the overall security operations. The Commonwealth Government has established special arrangements for coordinating its Games security responsibilities. The structure is based on a Ministerial Sub-Committee on security, supported by the Secretaries Committee on National Security. Since February 1998 the

Sub-Committee has been serviced by a newly-formed Sydney 2000 Games Coordination Task Force (located in the Department of the Prime Minister and Cabinet). The Task Force was responsible for the higher-level policy coordination for both security and non-security issues in relation to the Olympic and Paralympic Games. The Protective Security Coordination Centre has been working in close consultation with the Task Force on security aspects. A variety of coordination and consultative mechanisms have been set in place to enable Commonwealth and NSW Government agencies to work together in developing joint plans and procedures. Figure 11 represents the Commonwealth Olympic Coordination Arrangements.

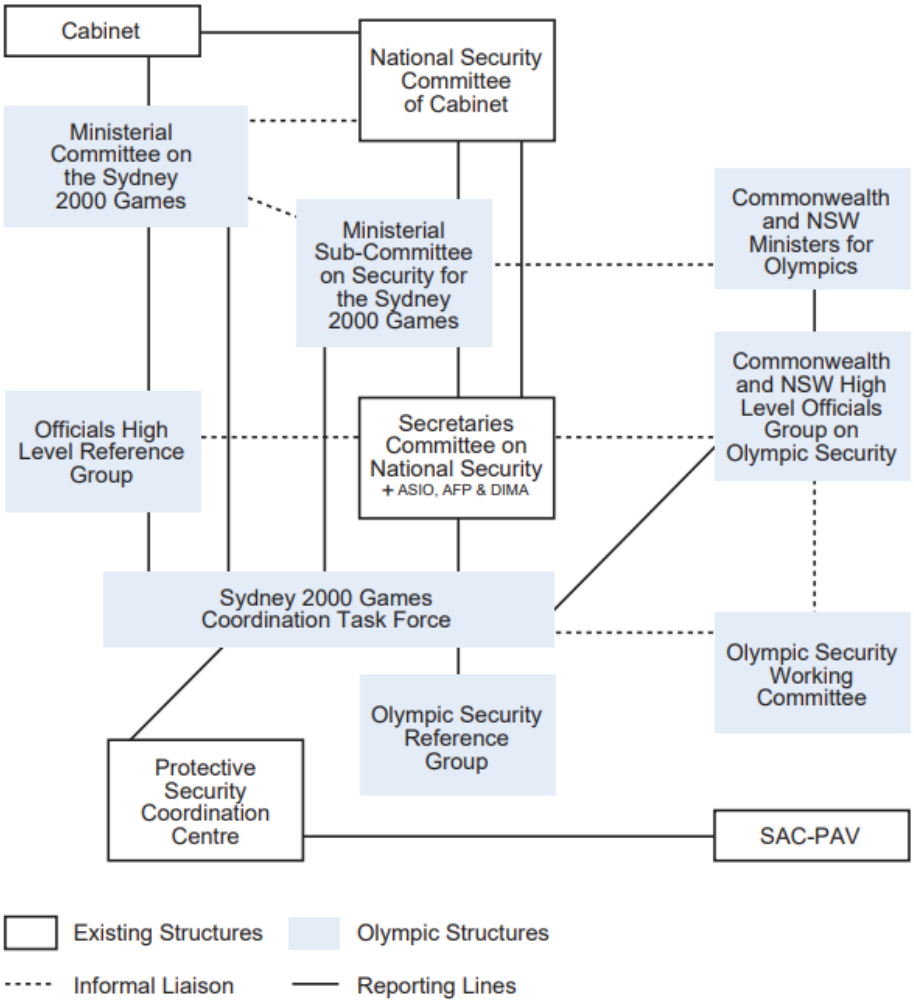


*Figure 11: Commonwealth Olympic Coordination Arrangements (Australian National Audit Office's Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games, 1998)*

According to the Australian National Audit Office's Commonwealth Agencies' (1998) security included: law enforcement - community policing (public order, traffic management, response capabilities); criminal investigation; protective security - personal protection; venues and facilities; movement security; information security; national security elements - coordination and planning, intelligence services; border management

and aviation security; security related services - Defence Force Aid to the Civil Power, Defence Assistance to the Civil Community; technical surveillance capabilities; and secure communications.

In terms of personnel, Sydney OC deployed approximately 5 000 police, 3 500 defence and up to 7 000 contract security staff (Lenskyj, 2002). According to the Australian Security Intelligence Organisation - ASIO (2000) the Sydney Olympics was the main focus of ASIO's work in 1999/2000, emphasizing at the same time the following:

- An intensive three-year program of preparations for the security of the Games was finalized and the Federal Olympic Security Intelligence Centre was activated on 1 May 2000, which issued 82 Security Situation Reports, each of which addressed multiple security issues.
- By 30 June the ASIO had provided security assessment advice to NSW Police on 62 167 people accredited to the Olympics (including SOCOG employees). Their updated counter-terrorism technical capabilities were successfully deployed with NSW Police and the Australian Defence Force in national counter-terrorism exercises.
- Additional direct electronic links were established with liaison partners. The links were relevant to Olympics security and are planned to be of continuing value in counter-terrorism.
- A key challenge in 1999/2000 was the recruitment and integration of significant numbers of temporary staff to meet the Olympics workload.

- The ASIO provided more than 157 000 Olympic-related security clearances for people accredited to the Games and for the entry into Australia of some Olympic Family Members.
- The ASIO issued 423 threat assessments specifically related to Olympics security.
- The ASIO interviewed 57 people of specific security interest to assist in the prevention of politically motivated violence during the Olympics.
- During 1999/2000 the following analysis and advice contributed to reducing the threat from foreign influenced politically motivated violence: a) Forewarning of potential threats to Australian high office holders and minority communities; b) Forewarning of potential threats to the Olympic Games which provided a sound risk management basis for security planning and was welcomed by NSW Police, Victoria Police and other clients.
- During 1999/2000 surveillance operations were primarily focused on groups or individuals assessed as a potential threat to the Sydney 2000 Olympics.

According to the Australian Security Intelligence Organisation (2000), over the reporting period the ASIO have participated in SAC-PAV counter-terrorism exercises with police services in New South Wales, Victoria, South Australia, Western Australia and the Australian Capital Territory. Those activities have strengthened their relationship with the NSW Police in the lead-up to the Olympics, conducting joint exercises, including the Technical Support Unit, to ensure integration and interoperability. The ASIO worked with other Commonwealth and State authorities and the Australian Defence Force to improve

and integrate capabilities before the Olympics. The exercises provided a valuable opportunity to test counter-terrorism response capabilities prior to the Olympics. Rigorous post-exercise reviews have enabled the ASIO to refine capabilities further. The ASIO contributed also to a review of the NATP, coordinated by the Protective Security Coordination Centre. The aim of the review was to amend policies and procedures to enhance national capabilities to respond effectively to contemporary trends in terrorism.

The Australian Security Intelligence Organisation (2000) emphasize a major challenge in recruiting experienced and capable temporary staff to meet the Olympics workload and replace separating staff. There were 60 separations in 1999/2000, out of a workforce of 605 staff. 52 of the 60 were permanent officers and 8 were temporary employees.

Additionally, the Olympics accreditation checking was facilitated with the development of a Bulk Automated Name Checking System, and an electronic link allowed the NSW Police to send batches of names to ASIO electronically. This enabled the ASIO to check large numbers of names through their index without a significant increase in staff (Australian Security Intelligence Organisation, 2000).

In contrast to previous approaches, the Australian authorities put great effort into surveilling Olympic visitors within and outside the Olympic venues. New surveillance cameras (CCTV), computer networks, satellites and other technologies were installed to undertake the surveillance efforts. For the first time the security operations were also criticized heavily in the run up to the Olympic Games. The Australian anti-Olympic

groupings were concerned about the surveillance and disturbing securitization of Sydney´s citizens (Lenskyj 2002).

Security costs for Sydney's Games totaled 250 million $ (Matheson, 2013). Toohey and Taylor (2012) highlight some of the security legacies that followed the Sydney 2000 Olympic Games, including enhanced capacities for surveillance and legislative powers for police and security agencies to control and monitor behavior at localized sports events. Whilst no significant security incidents occurred in Sydney, the surveillance infrastructure was kept after the Olympic Games (Toohey and Taylor, 2012). Although from a security point of view the Sydney 2000 OG passed in a calm tone, in the context of these event it is worth mentioning that the New Zealand police uncovered a possible plot to blow up a Lucas Heights nuclear reactor near Sydney during the Olympic Games (International Institute for Counter-Terrorism, 2000).

## 4.2 CASE STUDY: ATHENS 2004

The 2004 Olympic Games in the Greek capital were the first summer Olympics post-9/11, while Greece was the second smallest country to host the Games. According to Migdalovitz (2004) Greece's record in combating domestic terrorism was widely regarded as deficient. A group called the Revolutionary Organization 17 November (17N) had acted with impunity since 1975, claiming responsibility for assassinating four US officials and many others. Following the fortuitous arrest of a 17N terrorist in June 2002 after a bomb exploded in his hands prematurely, Greek authorities captured suspected leaders and members of the group. There have been no reports of radical Islamist terrorist groups operating in Greece, but police surveillance of Muslims reportedly has been increased in anticipation of the Olympics (Athanasidis, 2004). Regarding the international threats, it is important to emphasize that the alleged Al-Qaeda links to the November 2003 bombings nearby Istanbul and the March 11 2004 bombing of a commuter train in Madrid have heightened the Greek government's already keen awareness of a possible international terrorist threat to the Olympics (Migdalovitz, 2004). Both athletes and officials raised concerns about the possibility of terrorism via the media and spoke about the emotional effects that these threats were having on their preparations (Kennelly, 2005).

At the political level the Olympic Security Plan was assumed by the Minister of Public Order, and, at the strategic-operational level, by the Chief of the Hellenic Police (Ministry of Public Order Press Office, 2004). The government has created a special Coordinating Council for Olympic Security, consisting of ten ministers and chaired by the Minister of Public Order (Migdalovitz, 2004). These Games were a kind of step forward

in terms of formally structured international cooperation. Greece had to build an international security alliance and purchase the latest technology made in the United States and the European Union to get support and confidence, regardless of the expenditure (Samatas, 2007). In 2000, the government established a seven-nation Olympic Advisory Group from Australia, France, Germany, Israel, Spain, the United Kingdom and the United States (headquarters in Athens). For example, the US contribution involved the CIA, the FBI, State, and Defense Departments. Olympic Advisory Group members have participated in training Greek Olympics security forces, focusing on the potential for transnational terrorism. For example, Israeli specialists conducted training on identifying and neutralizing suicide bombers (Migdalovitz, 2004). Greece also received security advice from governments outside the Advisory Group, notably Russia, with whom was arranged the sending mobile laboratories to help in the event of a nuclear, biological, chemical attack and putting special forces on standby to deal with a possible Chechen threat (Migdalovitz, 2004). According to Migdalovitz (2004) Greece requested even NATO[3] assistance (AWACs planes for air policing and for dealing with a possible air attack; the Standing Naval Force Mediterranean to patrol extraterritorial waters around Greece; assistance with nuclear and biochemical defenses; and intelligence). The UN International Atomic Energy Agency was providing advice and equipment related to radiological dispersion devices. Additionally, the Athens government signed 32 special bilateral agreements with each of its closest neighbors in the Balkans, Mediterranean and

[3] Most of the high-tech security in Athens, especially military hardware, was borrowed from the US or NATO (Brianas, 2004; Lynch and Cuccia, 2006).

southeastern Europe in an effort to address issues which might arise in connection with the event (Voulgarakis, 2005).

According to Migdalovitz (2004) the Greek government contracted with the US-based Science Applications International Corporation (SAIC) to provide components of the security infrastructure for the Olympics at a cost of about 250 million $. SAIC headed an international consortium helping Greece with security that includes Siemens, Nokia, AMS, E Team, and the Greek companies ALTEC, Diekat, and Pouliadis-PC Systems. SAIC was building security command centers for the government to connect the police, the national first aid center, fire department, coast guard, and armed forces, and creating security systems, mainly surveillance equipment and management.

According to the Ministry of Public Order Press Office (2004), the Olympic Strategic Security Command Center (OSSCC) was based at the premises of the Ministry of Public Order, and operated on a 24-hour basis (51 officers from all main Security Forces). The Olympic Strategic Security Command Center was fully interconnected with the OSCC and has been receiving data and information from all over Greece. The OSCC was the "knowledge" center and also the coordination and administration center of all Olympic Security Operations. More than 750 officials from all the involved agencies were assigned in the OSCC. The Crisis Management Room was based at the OSCC. The Olympic Intelligence Center has been operating on a 24-hour basis since July 1st 2004. It represented the reference point and the unique central channel of information of Olympic interest. Daily, it provided risk assessment based on the information and the evaluation

provided not only by National Intelligence Services but also by other domestic and foreign channels of information.

The Athens 2004 Olympics became the testing ground of the latest antiterrorist surveillance technology, while Athens appeared to be a defensive fortress during the games (Samatas, 2004). The design of the Athens 2004 Olympic security project, characterized by the American Society for Industrial Security (ASIS) as the biggest security operation in peacetime Europe, aspired to work as a "superpanopticon". This meant a super electronic surveillance system providing the possibility of continuous online linking and processing, evaluation, classification, and identification of personal data, and the production, even simulation, of various personal information profiles for a variety of purposes (Norris and Armstrong, 1999). According to ASIS (2006) the Athens 2004 Olympic superpanopticon was prescribed to include a large-scale surveillance integration security network composed of 29 subsystems integrated into a unified command and control system linking the Greek police, firefighters, the Greek Coast Guard, and the Greek Armed Forces through 130 fixed and five mobile command centers. Information data were provided to a 7 000-strong Greek security force guarding 39 Olympic venues and critical infrastructure facilities, such as power stations, water works and fuel depots (ASIS, 2006). This Olympic superpanopticon was perceived as an electronic nexus of cameras, vehicle tracking devices, blimps, AWACS airplanes and satellites with continuous online linking by common databases and communications to provide real-time images and updates of available resources to a central command (Samatas, 2007). The major systems for the Athenian Olympic panopticon were based on the SAIC-Siemens security consortium of international corporations, which had

to provide high-tech panoptic technologies. A super surveillance project prescribed a network of 1 250 to 1 600 interconnected CCTV cameras installed all over the Athens metropolitan area, running 24 hours a day (Samatas, 2007).

According to Samatas (2007) the Greek government created an initial 800 million € security budget for the Games security. Of that, they commissioned 255 million € to the Command Control Coordination Communications & Integration (C4I). Thus, the SAIC consortium was awarded the bid for the central security system. This later escalated into a scandal, as the organizers did not have the planned benefits of the system (Samatas, 2014). According to the Ministry of Public Order Press Office (2004), the C4I systems are technological means of communication, data processing and security that are completely interactive and provide information (image, sound, data) to authorized law enforcement commanders, allowing the latter to evaluate a situation in real time and to facilitate decision-making. The C4I systems include:

- Specialized Security Systems;
- Systems of physical Security;
- Digital multi-channel radio network of Olympic Security;
- Construction and equipment of Operational Centers (regular and mobile);
- Systems of Information technology.

The C4I systems, through thirty sub systems, had to allow a concise image of multiple incidents at any given time by combining: Air surveillance; CCTV cameras; AVL (automatic vehicle localization); Command Centers; Port Security Systems; Fire

Surveillance Systems. 4 000 officials from the Hellenic Police, the Coast Guard and the Fire Brigade, the Armed Forces, the National Emergency Response Center, the Customs and other involved Agents were trained in these systems (Ministry of Public Order Press Office, 2004).

According to the Ministry of Public Order Press Office (2004), the Mobile Operations Center "Alexander the Great" was one of the mobile operations centers of the Hellenic Police and a part of the C4I project. The task of the "Alexander the Great" was to support the assignment of Operation Commanders of the Hellenic Police during the management of serious security incidents or crises, in Olympic cities or anywhere in the country, wherever organized Operation and Communication Centers are not available. According to the Ministry of Public Order Press Office (2004) the Air Operations Coordination Center was responsible for air surveillance while the Hellenic Police Air Force Service allocated helicopters (type BO-105 and EC-135) and pilots and technicians, with main assignments:

- The transportation of Police officers in case of emergency;
- The transportation or escort of VIPs;
- The transportation of patients or wounded;
- The assistance in regions affected from calamities and grave accidents;
- The transmission of data and image to TCMOR and the respective Police Forces for policing tasks (e.g., for traffic management, transportation safety etc.);
- The operational support to Special Police Services (e.g., Special Counter Terrorist Unit, Special Violent Crime Squad etc.).

Around 70 000 military and security staff went on patrol by the start of the Olympic Games (Samatas, 2007). A secure and efficient communication system is one of the fundamental infrastructural components of the overall security and safety of mass gatherings. According to the Ministry of Public Order Press Office (2004), the Terrestrial trunked radio system (TETRA) was planned as the main communication tool of Road Traffic Police as it supports a total of 1 000 communication groups from the Agencies assigned with Olympic duties: The Hellenic Police, the Armed Forces, the Fire Brigade, the Coast Guard, National Center for Emergency Response and other Agents. TETRA provides:

- Unified and efficient communication;
- Capacity of access to information systems;
- Encrypted, safe transmissions;
- Interoperability with all the Involved Agents and Services;
- Multi user connection, even during the incident development;
- Exclusive communication without interjections, at a group level or between individual users;
- Reliability and Interconnection with data base.

The figures 12 and 13 presents the C4I concept overview and airborne video surveillance system.


*Figure 12: C4I concept overview (Siemens, 2007)*


*Figure 13: C4I airborne video surveillance system (Siemens, 2007)*

However, as Samatas (2007) explains, the much-lauded C4I system was not delivered on time for the Olympics. Actually, it not only did fail to work during the Games (or after-in fact, it never worked as an integrated system), but it also implied several other related serious scandals, such as bribes to the Greek ruling parties of New Democracy and PASOK, as well as prolonged phone tapping of the Greek government (Samatas, 2014). Nevertheless, the Games proceeded without major incident. The failure of C4I had no impact on safety, but it was a massive security failure to the degree that the flash of the Olympics could only be met by the low-tech thud of soldiers' boots (Samatas, 2007).

Rising costs proved an extreme challenge for a financially weak country like Greece (Krieger, 2019). Security expenditures topped 1.5-1.6 billion USD, four times the initial budget (Matheson, 2013). Applied measures suggest that Athens was the most guarded Olympic Games until that moment (Wilson, 2004). Still, much of what the Greek government sought in the costly C4I system was for post games use. For example, a few months after the Olympics, there was a Greek Police post-Olympic success when police persuaded two gunmen to surrender after a hijacking (involving 23 hostages) with a methodical operation born of Olympic experience (Samatas, 2007).

## 4.3 CASE STUDY: BEIJING 2008

Political scientist Yu et al. (2009) has described the 2008 Beijing Olympics as the largest peacetime security operation in history. According to Yu et al. (2009), in the months leading up to the 2008 Olympics, the Chinese media reported at length a wide range of threatening forces to the Games:

1) Terrorism, described as the most critical security issue at the Games. "Xinjiang independence" organizations were treated as the most dangerous terrorist enemies to Olympic security.
2) Various forms of criminality, both indigenous and foreign originated, ranging from petty crimes, frauds, rapes and kidnappings to internationally organized crimes and people trafficking (prostitution and labor).
3) Sabotage activities of Tibetan independence organizations were not only seen to endanger the athletes and population, but also to threaten the carefully constructed image of the Olympics as a symbol for China's unity and rising power in global affairs.

Security governance for the Beijing Olympics was quite a complex. According to Yu et al. (2009) security governance has focused on specific points within the urban environment, corresponding both to central, interrelated nodes within the Beijing transport networks such as airports and railway stations and to high-risk points such as stadiums and hotels for International Olympic Committee officials. Yu et al. (2009) added that Beijing's security strategies have dwelled in a distinctive authoritarian political system, with the government asserting strong control over the involvement of international security players.

However, the potential of local crime was under the magnifying glass. The security operations in Beijing focused on two main aspects: removals and military operations. Their efforts included the removal of local criminals and robbers as well as the confiscation of illegal explosives, guns and ammunition (Yu et al., 2009). The Chinese Security Ministry explained approach as a "sand-pile effect", meaning that the fight against petty crimes and minor problems of disorder, as the basis of the sand pile, would help to reduce major threats of criminal and terrorist activities, i.e., the peak of the pile (Security Command Centre for the Games of XXIX Olympiad, 2007). According to Xinhua News (2008) zero-tolerance repressive strategy was also applied to common criminal cases in the ongoing "strike hard" campaign against crimes, as programmed in the so-called "Action for a Safe Olympics". From January to May 2008, Beijing police forces beefed up security for the Olympics by cracking down on organized crimes, robbery, murder and other severe criminal offences, confiscating illegally held explosives, guns and ammunition, strengthening control over knives, bows and crossbows. They also stepped-up surveillance on entertainment venues to fight pornography and gambling.

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. On a regional scale, exchanges were intensified among police agencies in China, Japan and South Korea (Yu et al., 2009). In 2005 the International Permanent Observatory on Security Measures During Major Events was established, bringing together 24 foreign security experts from ten countries and four international organizations, including the US Federal Bureau of Investigation, the United Nations' Inter

Regional Crime and Justice Research Institute and the European Police Office, in order to share their experience at earlier events such as previous Olympic Games, the 2004 European Football Cup and the 2003 Evian G8 Summit (China Daily, 2005). In order to learn from the experiences of previous mega-events, Chinese security officials participated in 'best practices' training programs with security stakeholders at earlier events, receiving training in violence prevention, policing management and information management in police colleges in Britain, Germany, Australia and other countries (The First, 2005). In addition, 39 Chinese officers were sent to Greece to learn from the Athens Olympic security model (Xinhua News, 2005). Beijing also established a "Memo of 2008 Olympic Games and Paralympics on Security Cooperation" with the Ministry of Hellenic Public Order in Greece (Promotion Film for the Security of Beijing Olympics, 2007). To coordinate the international efforts in the Games' securitization, an International Police Liaison Department was established within the Security Command Centre to coordinate interactions between embassy security officers, police departments from other countries and international police/intelligence organizations (Xinhua News, 2007). The Chinese national army, navy and air force participated fully in the 2008 Beijing Olympics security work, with the establishment of a special military unit for non-traditional security threats focusing on threats of nuclear, bio-chemical and other terrorist attack (Xinhua News, 2007).

According to Mulvenon (2008), the People's Liberation Army (PLA) support falls into roughly two categories: Olympics preparations and security work. Chinese media report that in the Olympics the People's Armed Police (PAP) is primarily in charge of 12

security tasks: standing on the alert and guarding Olympic competition venues; standing on the alert and guarding Olympic training venues; standing on the alert and guarding non-competition venues; maintaining the security at the Olympic Opening, Olympic Cultural Festival, and other large-scale activities; guarding lodgings, activity routes, and activity sites of VIP's; guarding lodgings, activity routes, and activity sites of members of the International Olympic Committee; guarding Olympic torch relay sites and routes and escorting the protocol of the torch; guarding award-presenting distinguished guests; standing guard at the periphery and sites of Olympics-related airports and safeguarding special planes; safeguarding water, electricity, gas, oil, communications, and other pivotal facilities closely related to the Olympics; checking and publicly patrolling key business districts; and handling sudden incidents and countering terrorism and hijacking; as well as four volunteer tasks such as delivering medical aid in the Olympic Village (Zhang and Zhang, 2008). According to Mulvenon (2008) within the Games itself, the roles of PLA are varied and specialized. PLA units were responsible for six tasks: (1) aerial security in Beijing and competition areas outside of Beijing; (2) maritime security on the sea close to the coastal area; (3) handling nuclear, chemical, and biological terror attacks, and assisting the public security department in handling terror events such as explosions; (4) intelligence support; (5) emergency rescue, medical rescue and helicopter transportation, etc.; and (6) border control during the Olympic Games to maintain stability along the border and in coastal areas.

According to Yu et al. (2009) a specialized security department and command center for the Olympics was established directly under the state ministry of public security,

involving over 20 related state and municipal ministries/departments, including the military. Force estimates vary, but official statements from 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 (Mulvenon, 2008). According to the United Nations Office of Counter-Terrorism Guide on the security of major sporting events (2021) China's effort to make the "high-tech Olympics" included approximately 265 000 new surveillance cameras covering more than 50% of Beijing, and even inserting RFID chips into tickets to provide security screeners with the bearer's name, address, e-mail, phone number and passport details. According to Yu et al. (2009) high-tech surveillance systems were delivered by United Technologies, the European Aeronautic Defence and Space Company, Panasonic, Philips, JVC and Siemens. Besides international technology providers, national and local companies also played an active role. According to Xinhua News (2008), an extra 2 000 cameras, partly equipped with face and license plate-recognition software, were installed in the Chaoyang district, covering 54.2% of the district's surface by CCTV.

According to Yu et al. (2009) the securitization of the Beijing games relied on a wide range of preventive security measures. Before the event, surveillance and control had increased substantially, based not only on the wide use of security technologies in Beijing itself but also on international exchanges of databases of criminal and terrorist suspects. The expert conferences and "best practices" programs discussed earlier not only served to institutionalize the practices and relationships underlying the securitization of the event itself, they also provided a space of experimentation to adjust and rehearse the uses of the

newly installed high-tech security systems. Beijing deepened grassroots security operations by promoting education on public safety and crime prevention, inciting social groups and the general public to watch their neighborhoods, care for their home and do everything they could to participate in the Olympic Games security work (Xinhua News, 2007).

The Security Industry Association (2007) estimates that China spent 6.5 billion USD on security-related projects across Beijing that were not part of the budget for the Games but still timed to coincide with the event. Despite a number of minor cyber-related attacking attempts, the Games passed without a single major security incident.

## 4.4 CASE STUDY: LONDON 2012

British authorities recognized terrorism as the major threat to security, placing this ahead of serious crime; domestic extremism and public disorder; natural hazards (London 2012 Olympic and Paralympic Games Quarterly Report, 2012, October). Also, for the first time in history, a special emphasis on IT security has been witnessed within the security preparations for the Olympics. A large part of the concerns was triggered by the terrorist bombings that occurred in London on July 7 2005, killing 52 people and injuring more than 700 (Krieger, 2019). The attack took place the day after London had been awarded the 2012 Olympic Games and created a constant public link between terror and the Games. According to London 2012 Olympic and Paralympic Games Quarterly Report (2012, October) the management of the Olympic and Paralympic Safety and Security Programme, which covered policing and wider security for the Games, was the responsibility of the Home Office. The Home Secretary was the lead minister, accountable for the delivery of the Safety and Security Strategy and the Security Programme as a whole. The Office for Security and Counter Terrorism (OSCT) within the Home Office, managed the strategy and its associated programs, and ensured their delivery through the police and other agencies, departments and organizations. The Government's approach was intelligence-led and risk-based, ensuring flexibility to respond to changes in circumstance. The planning assumption used throughout was that the Games would be delivered in the context of a "severe" level of terrorist threat, higher than the "substantial" level experienced in the run up to and during the Games. According to London 2012 Olympic and Paralympic Safety and Security Strategy (2011) the Olympic Security Board (OSB), provides collective senior

official ownership and oversight of the Strategy and its associated plans and of the residual risks. The OSB includes those responsible for:

- delivery of major components of the Programme;
- funding for major components of the Programme, including changes to funding as the Programme proceeds;
- delivering other components of the Games which have a major dependency on its security and safety;
- assessing or recommending the impact of changes (e.g., a change in threat assessment).

According to London 2012 Olympic and Paralympic Safety and Security Strategy (2011) the Olympic and Paralympic Security Directorate is mentioned to:

- be the agent for the Government's guarantee of a safe and secure Games;
- maintain the Strategy and the overarching Safety and Security Concept of Operations;
- oversee the budget and the Programme of capability enhancement;
- manage the coalition of delivery partners needed to fulfil the Guarantee;
- monitor progress and communicate it to Ministers and beyond;
- ensure that the capabilities, plans and operational measures are fully tested and evaluated;
- resolve problems that may impede the delivery of the guarantee;
- ensure that the legacy and wider benefits of Games security are realized.

Figure 14 presents an interrelation of security-related activities within the London 2012 Olympics.

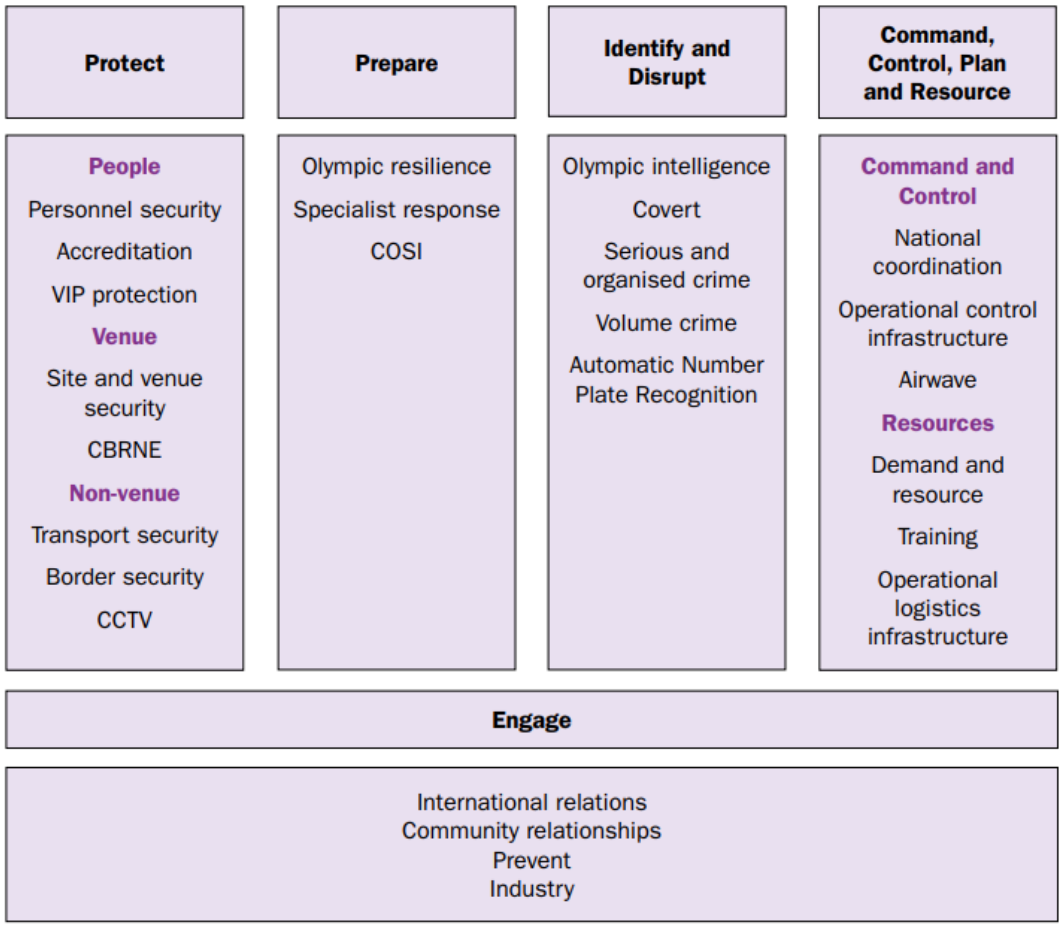


*Figure 14: Interrelation of security-related activities within the London 2012 OG (London 2012 Olympic and Paralympic Safety and Security Strategy, 2011)*

According to Coaffee et al. (2011), in addition to proactive policing and intelligence efforts being directed towards potential threats, key elements of the total security model included at least three key stages. The first involved intense planning for "resilience"

should the goal of "prevention" fail and security problems such as a terrorist attack eventuate during the Games. The second involved reconfiguring public and private space into security infrastructures through the development of "island" security and sophisticated "defensible space" techniques at key sites. The third concerned the deployment of advanced surveillance and real-time monitoring of people and space, much of which involved expanding the existing network of surveillance technologies in the host city. These measures were also accompanied by an intense "military urbanism" that played a crucial role in the overall "securitization" of the Olympic Games. A ring of steel has been created around the Olympic village and sports venues. 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 (army, police, special forces) and their visibility, extensive installation of digital video surveillance (Bilandžić and Leško, 2019). In view of such, it was almost impossible for critics to argue against supersize security to respond to the potential terror threats (Sugden, 2012). A total of 89 000 police officers were on duty every day during the Games (Fussey, 2015), while total number of defence personnel was approximately 17 000 (Hopkins and Booth, 2012).

In a personnel context London 2012 noted a serious failure that did not pass under the public radar. In December 2010, the venue security contract was awarded to the G4S. The G4S was contracted to recruit, train and accredit 10 400 staff and manage 13 000

others. The total number of security personnel required for the Games was 23 700. According to the House of Commons Home Affairs Committee Olympics Security Seventh Report of Session (2012-2013), the running of the Games was thrown into serious doubt two weeks prior to the Opening Ceremony when the principal security contractor, G4S, suddenly announced that it would not be able to fulfill its contractual duties. In the following days leading up to the Opening Ceremony, G4S's inability to deliver to its contract became the largest challenge facing the London OC of the Olympic and Paralympic Games. Thanks to robust contingency planning from an early stage, and the recognition by LOCOG, Home Office officials and the police that the problem might be far worse than G4S initially suggested, arrangements were quickly made for armed forces personnel to fill the gap left by G4S's shortfall. According to the House of Commons Home Affairs Committee Olympics Security Seventh Report of Session (2012-2013), total military deployment for the Olympic Games peaked at 18 200 troops (the original target military workforce was 7 500), while additional police manpower was provided to fill the gap left by G4S through officers working overtime.

According to Dion-Schwarz et al. (2018), dubbed the first digital Olympic Games, they were the first summer Olympics to take place in the smartphone era and saw unprecedented use of Wi-Fi and mobile services (including the world's largest high-density Wi-Fi network, installed by BT and Cisco around Olympic Park). London 2012 undertook a multipronged cybersecurity strategy that included a 30-point cybersecurity action plan. The Olympic Cyber Coordination Team, the first "Olympic CERT", brought together representatives from the Home Office, Ministry of Defence, Security Service/MI5, Cyber

Security Operations Centre, Government Communication Headquarters, and Centre for the Protection of National Infrastructure. The Technology Operations Centre, operated around the clock by the London Organising Committee's IT team, was jointly staffed by BT, Atos, and Cisco and had secure, direct communication lines to the Olympic Cyber Co-ordination Team (Dion-Schwarz et al., 2018). Overall, London 2012's cybersecurity efforts were considered a success, and the Games saw only low-level cybersecurity incidents. There were no successful high-profile, high-impact events. Of an estimated 165 million "security-related events", the 2012 Olympics chief information officer Gerry Pennell (2013) reported that 97 were serious enough to be referred to the Technology Operations Centre, and only six would have had a major operational impact on the Games. A few of them are listed (Dion-Schwarz et al., 2018 according to Pennell's speaking at a cybersecurity event in 2013 and other newspapers releases):

- On July 26 (the day before the Games opened), a high-profile group of Eastern European hackers probed London 2012's IT infrastructure for roughly ten minutes. The group has a history of publishing the vulnerabilities of high-profile websites; however, in this case, "they didn't find anything," and no vulnerabilities were published.
- July 27 saw a massive 40-minute DDoS attack on the Olympic Park's power systems starting at around 5:00 PM, with an estimated 10 million requests originating from 90 IP addresses in North American and Europe. This automated botnet-style attack failed and was likely intended to disrupt the opening ceremony.

- Additionally, it was reported in multiple media outlets that there was a suspected state-sponsored cyberattack.

Former London 2012 cybersecurity head Oliver Hoare (2018) identified what London 2012 got right on cybersecurity:

- Testing and exercises to ensure cybersecurity preparedness;
- Contributions by the Olympic CERT to command, control, and communication capabilities (though it would have been better if a UK CERT had been in place beforehand);
- Allocating resources ahead of time;
- Cooperating with industry partners, such as BT, Cisco and ATOS;
- Coordinating and collaborating with broadcasting organizations (subject to critical threats) and utilities (subject to low-level threats with a potentially high impact).

Hoare (2018) also identified key lessons and areas for improvement:

- Understand that ICT is very expensive, particularly when it must be retrofit. The lesson is to aim to get it right first time and ensure that cybersecurity considerations are accounted for even in the requirements and procurement stages.
- Start planning early so that it is possible to build in cybersecurity and information assurance from very beginning, preferably in the contract phase; establish senior leadership and governance earlier; and engage sooner with ministers and other government leadership.

- Build relationships with commercial providers and government early.
- Coordinate across many different systems and sectors (via the Information Assurance and Cyber Security Coordination Group/ Senior ICT Group/Olympic Cyber Coordination Team). This step is difficult but crucial to successfully detecting and mitigating cybersecurity threats.
- Consider cyber incidents and issues in insurance terms. For example, what will it cost if media outlets lose the ability to broadcast?

Although exact expenditures vary among academic publications, it is estimated that the security costs for London 2012 were at least 950 million USD, despite the host city's already significant investments in security and surveillance infrastructure post the 7 July 2005 bombings and economic problems following the global financial crisis (Fussey and Coaffee, 2012a). Some reports indicate that the total costs for securing the 2012 London Olympic Games were as high as 3.1 billion USD (Houlihan and Giulianotti, 2012). This accounts for between 15 and 20% of the total costs for staging the Olympic Games. The security operation at the Games passed off without any significant problems, and the contribution of the armed forces and volunteers to the Games was widely praised. It was just as well in the circumstances that the military and police were able to be made available in view of the failure of G4S (The House of Commons Home Affairs Committee Olympics Security Seventh Report of Session, 2012-2013).

## 4.5 CASE STUDY: RIO DE JANEIRO 2016

The Olympic and Paralympic Games in Rio de Janeiro 2016 were the first held in South America. Already in the official bidding documents, the Bidding Committee had shown much awareness for potential security concerns with great emphasis on promising safe Olympic Games (Barbassa, 2017). Brazil´s economic crisis and politically unstable situation led popular demonstrations and civil disturbances to become a major concern for the authorities (Visacro, 2017). In the context of terrorism, in April 2016, Brazil's Director of Counterterrorism in the Brazilian Intelligence Agency, Luiz Alberto Sallaberry, was reported as noting that the threat of terrorism had increased in recent months due to attacks in other countries and a rise in the number of Brazilian nationals suspected of sympathizing with Islamic State militants (Rodrigues, 2016). The statement from Sallaberry was apparently in response to information related to a Tweet from November 2015 by a suspected ISIS executioner, who stated "Brazil, you are our next target" (Reuters, 2016). This warning came a year after a Brazilian newspaper reported that Brazilian intelligence agencies are gearing up to monitor people who may be enticed by online ISIS propaganda to perform "lone wolf" attacks (Martel, 2015). Ahead of the 2016 Rio Olympic Games, Brazilian police arrested twelve people suspected of planning terrorist acts during the time of the Olympics (Yan et al., 2016).

Bitencourt (2011), however, considered two distinct levels of threats when analyzing security prospects for the 2016 Olympic Games: the first is represented by the current domestic threats associated with crime and local violence that have been haunting Rio for many decades vis-à-vis the ability of the State to reduce and control exposure of

this threat to the sporting events, the athletes, and the public; and the second is represented by the prospects of a terrorist attack during the Games, when the target will not necessarily be Brazil, but the Games themselves, and/or specific country delegations. To face the first level of threat, Rio's authorities have considerable experience and have been implementing a robust set of measures that should result in an improved security environment by 2016. In an attempt to combat the domestic violence, the City of Rio de Janeiro demolished residencies in unsafe areas, in particular within the Favelas (Freemann and Burgos, 2017). According to Bitencourt (2011), the second level, however, has a much more prominent international dimension and requires a strategic approach. On the one hand, Brazil does not figure among the usual targets of current terrorist organizations, the most notorious being those espousing Islamic extremism. Indeed, Brazil has thus far neither been threatened with nor been the target of terrorist activity, which lends some assurance to the organizers of the 2016 Olympics. On the other hand, this reality may exactly suggest to terrorists that Rio might therefore act as an ideal operational environment for the perpetration of terrorist attacks. Bearing this scenario in mind, Brazilian police forces are not geared towards this type of threat and its prevention, presenting a dilemma to those who responsible for the security of the 2016 Rio Olympic Games.

Construction problems led to another security challenge. According to Lechner (2014), as it turned out a construction crane collapsed and fell into the almost finished Arena Corinthians in Sao Paulo, which later hosted the opening game of the Football World Cup. The collapse of this stadium was not the first incident during the preparation of both World Cup and the Olympic Games. A part of the roof collapsed from the weight of water

at Salvador's stadium. Another stadium, which hosted the Olympic athletics event, was closed down several months in fear of the roof collapsing and a further worker died at the new Palmeiras stadium earlier that year.

Further, in 2009 no one expected the outbreak of the mosquito-borne Zika virus in late 2015, when Brazilian health officials noticed an increased number of infants born with microcephaly. Although some have called for the Games to be postponed or cancelled, the US Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO) have indicated the risk of international transmission due to the Games as low (Halchin and Rollins, 2016).

According to Winter (2016), the SPIS considered the following items as major risk scenarios that could affect the safety operation of the Rio 2016 Games:

1) acts of terrorism or sabotage of any kind;
2) violent actions committed during social events;
3) crime and urban violence;
4) commitment of the urban mobility system;
5) commitment of public health;
6) commitment of essential services;
7) cyber-attacks;
8) natural phenomena;
9) incidents and disasters.

According to Preuss et al. (2019), The Olympic Games in Rio de Janeiro experienced several changes in their master planning after being awarded the Games. The main changes in relation to the original budget were:

1) the impact of the adjustment based on Brazil's Consumer Price Index;
2) the inclusion of four new sports (golf, rugby, paracanoe and paratriathlon);
3) new technologies;
4) security;
5) average salary increases above inflation;
6) spending on usage and retrofitting of the Olympic Village.

Security has become an important expenditure issue at the Olympic Games, as it was in Rio (Preuss et al., 2019). According to the United Nations Office of Counter-Terrorism (2021), given the social tensions existing in Brazil, i.e., high rates of street violence and criminality, the country faced a significant challenge in guaranteeing the security of spectators, participants and all other individuals involved in the organization and implementations of both major sporting events. To this end, Brazil enacted specific laws attributing responsibilities, and enabling law enforcement and military forces to effectively operate within the particular context of a major sporting event. According to the IOC Candidature Acceptance Working Group (2008) the National Secretary of Public Security, reporting to the Ministry of Justice, is entrusted for the security of the Rio Olympic Games. According to Halchin and Rollins (2016), although public security is primarily the responsibility of Brazil's states, the national government was in charge of

ensuring security around the Olympic Games. The Brazilian government approved the Strategic Plan for Integrated Security (SPIS) through the Interministerial Ordinance No 1678 of 30 September 2015 for the Olympic and Paralympic Games in Rio 2016 (Brazilian Government, 2015).

According to Winter (2016) the principles underlying the conduct of the institutions participating in the planning and implementation of safety actions of the Games were:

a) Complementarity: the possibility of institutions with specific mandate to perform certain tasks to be supported by others, complementary and cooperative way, whenever circumstances require;
b) Cooperation: joint efforts and interests to achieve goal, task, purpose or common mission. It is obtained through the harmony of distinct elements efforts aimed at achieving the same end, and avoiding duplication of efforts, resource dispersion and divergence solutions. To optimizes results, increases the effectiveness of actions and avoids mutual interference, which does not characterize subordination between the institutions;
c) Discretion: to ensure low media coverage in the development of actions;
d) Efficiency: ability of an operation to fulfill, properly and with economy of means, all planned assignments;
e) Technical excellence: Training of the professionals involved to operate in a qualified way within international working standards and respect for human rights, taking advantage to do so, modern equipment and systems able to guarantee the provision of services at the highest level;

f) Integration: joint action, articulated and coordinated between agencies, directly or indirectly, participate in safety actions, respecting the specific legal responsibilities of those involved;
g) Interoperability: the ability of systems, units, forces and institutions to exchange information and services without compromising their functionality;
h) Situational leadership: temporary situation that assigns a consensus basis, to an institution that has legal authority to fulfill certain task, coordination of integrated actions, respecting the powers of the other bodies involved;
i) Respect for diversity and human dignity: Constitutional foundation that ensures the exercise of social and individual rights and freedom of a fraternal, pluralist and unprejudiced society.

The security presence was expected to comprise 85 000 personnel, including 41 000 military troops. About 67 000 security personnel were based in Rio de Janeiro while 18 000 were deployed to the other five cities hosting Olympic football tournament. According to Preuss et al. (2019) the Brazilian Ministry of Defence created the Special Advisory Committee for Major Events, to the Joint Staff of the Armed Forces, which used the Joint Operations Centre as the venue for coordination and monitoring of the action to be taken by Brazil's three armed forces. The Brazilian Intelligence Agency was defined as the centralizing entity to coordinate the work of all other entities of the Brazilian Intelligence System. It was responsible for preparing risk assessments, producing knowledge, preventing terrorism and disseminating information, through the National

Intelligence Centre and the Regional Intelligence Centres established in the host cities (Social Communication Secretariat, 2016). In order to undertake preventive measures to combat terrorism, an "Antiterrorism Law" was sanctioned in March 2016 as Brazil did not have any regulatory instrument to define terrorism previously in place (Visacro, 2017). Also, the Brazilian authorities also continued the trend of growing IT security and online security checks for all spectators of Olympic events as the Brazilian government attempted to check all names against a database of people with alleged terrorism links (Gregory, 2016).

According to Winter (2016), as the central organ of the Brazilian Intelligence System, the Brazilian Intelligence Agency (ABIN) mapped the hacker groups most likely to act on major events. Also monitoring of several suspected work was carried out, which prevented more than 40 000 people interested in work, participate and even watch the Olympics. The whole process had the support of various agencies of international intelligence as the CIA, the Mossad, the Russian intelligence, France, Germany and several Latin American countries. The ABIN confirmed that at least 30 intelligence agencies-maintained operations in Brazil and other 90 were part of a network of exchange of information of which Brazil is a member. For the Olympic period, more than 110 intelligence agencies have been installed in Rio de Janeiro. Intelligence activities were coordinated by the Games Intelligence Center (CIJ) of the Olympic Games Rio 2016. The site housed professionals of 82 government agencies and utility companies (transport, water and energy for example), attendance system and guard. In the CIJ, professionals of various public utilities and services agencies were meeting to exchange information on the

security of the Olympics. The main objective was to subsidize the axes defence and public security in the protection of the Olympic Games.

Analysis showed that Rio 2016 did face a wide range of cyber-related threats, several of which were described in a Booz Allen and Cyber4Sight study (2016):

- cybercrime, such as ATM card skimming and point-of-sale malware that can capture and duplicate credit and debit card information;
- scams, for example, fraudulent ticket sales for Olympics-related events, as well as fake websites used to collect and steal payment credentials and PII fake Wi-Fi networks-some disguised as official Rio 2016 networks-used to collect and steal PII or the exploitation of unsecured Wi-Fi networks;
- exploitation of online payment systems, which facilitated the theft of credentials and PII to convert funds into Boletos, a payment method used widely in Brazil, as well as the use of Boleto malware commit fraud;
- hacktivist activity in response to budget overruns during the 2014 FIFA World Cup that saw a resurgence in the months leading up to Rio 2016.

The Brazilian Network Information Center (NIC.br) is the executive branch of the Brazilian Internet Steering Committee and maintains the Brazilian National Computer Emergency Response Team (CERT.br). According to Dion-Schwarz et al. (2018) during Rio 2016, NIC.br and CERT.br were responsible for identifying potential threats and needs related to infrastructure and processes; collecting and monitoring incidents reported by stakeholders; monitoring networks and data feeds for defacement or intrusions, including

public sources of information, such as social media and public-facing websites; facilitating communication and coordination among various stakeholders, particularly CSIRTs, telecommunications companies, ISPs, hosting companies, and international partners; training incident handling teams; and maintaining the InterNetwork Operations Centre Dial-by-ASN (more commonly known as INOC-DBA), a VoIP network that enables communication among network operations centers, security incident response teams, and other essential personnel (Desiderá, 2016). According to Desiderá (2016) in total, four teams collaborated to prevent, identify, and respond to cyber incidents during Rio 2016:

1) Rio2016 CSIRT provided round-the-clock onsite support and handled incidents related to the Rio 2016 infrastructure, phishing attempts targeting official Rio 2016 websites, and websites selling fake tickets.
2) CERT.br coordinated and facilitated communication with external stakeholders, provided situational awareness, and conducted network monitoring. Incident reporters were encouraged to copy CERT.br on any notifications to Rio2016 CSIRT to support situational awareness.
3) CTIR Gov, a Brazilian governmental CSIRT, handled incidents that targeted networks belonging to the Brazilian Federal Public Administration.
4) Centre for Cyber Defence personnel staffed Rio 2016 security command and control centers on a continuous basis, focusing on the defense of critical infrastructure and networks of interest to the Brazilian Ministry of Defence.

According to Desiderá (2016) there were no high-profile, high-impact cyber incidents that negatively affected Rio's ICT infrastructure. Nonetheless, Rio2016 CSIRT and CERT.br did identify, observe, or respond to a number of lower-level incidents, including cybercriminals' exploitation of the games to attract financial fraud victims; unauthorized ticket selling on fake websites; hacktivism, including website defacements; data leaks from government and Olympics-related organizations; DDoS attacks against government and Olympic sponsors' websites, peaking at 300-500 Gbps.

In total, 895 million USD were spent on security for the 2016 Games (Guardian, 2016; Marketplace, 2016), noting that a significant part of the funds for security infrastructure was invested two years before for the World Cup. Kao (2016) states that construction for the Olympic Games Rio 2016 were subjected to even heavier scrutiny than for previous Games. There were protests over costs, while political unrest, a recession and environmental concerns drew attention to the vast construction undertaking, the cost of which made up a large portion of the overall Rio Games budget. Additional reasons for the cost overruns become obvious: political instability and, connected to that, a high level of corruption in Rio; recession, which meant budget pressure on the government and a higher unemployment rate; and environmental concerns, which may translate into additional expenditure to clean the water in Guanabara Bay or fight mosquitos (and fight the Zika virus).

## 4.6 CASE STUDY: TOKYO 2021

The peculiarity of the Tokyo Games is the fact that they were postponed for a year, due to the SARS-CoV-2 pandemic, which made risk management and overall security and safety more complex and more expensive. Additionally, the possibility of earthquakes in Japan is well-known. Concerns prevailed among the security community that a focus on the SARS-CoV-2 would not distract from preventing terrorism, the highest security threat to the Olympic Games. In 2013, Prime Minister Shinzo Abe held the Ministerial Meeting Concerning Measures Against Crime, where a draft *Strategy to Make "Japan the Safest Country in the World"* was discussed. From the beginning of planning, the Japanese planned visionarily. In a security and safety sense, the intensified measures for the Olympic Games should be used as a legacy to preserve the long-term security among the country. According to the IOC Candidature Acceptance Working Group (2008) the command and control of security forces is entrusted to the Superintendent-General of the Tokyo Police. The government itself was strongly involved, and special reliance was placed on strong private companies. According to Sugiyama (2020) the Security Strategy for the Tokyo Olympics was created in March 2017 (partially revised later). The main measures were planned to be promoted in cooperation with related ministries and agencies:

1) Ensuring the safety of the competition venues;
2) Ensuring the safety of athletes and spectators;
3) Ensuring the continuity of important services;
4) Border measures;
5) Strengthening the security of important facilities, soft targets, etc.;

6) Strengthening efforts to prevent terrorists from acquiring weapons;
7) Strengthening cyber security measures;
8) Strengthening international cooperation;
9) Responding to natural disasters;
10) Mentioning strengthening emergency response capabilities.

The revision included drone countermeasures, while the SARS-CoV-2 made security and safety plans more complex later on. Additionally, the organizers established a cooperation with the IAEA, on Nuclear Security at the Games.

According to Sugiyama (2020), in terms of security, Panasonic was the top-level partner with the highest level of sponsorship. The NEC was the second gold partner provided face recognition systems for access control (biometric authentication, behavior detection/analysis, drones) and network products (SDN, wired). The explosive-detecting system was developed by multinational company Hitachi, which is said to have paid attention to specific kinds of tiny particles that stick to hands or clothes after contact with explosives. That system is able to check up to 1 200 people per hour with Hitachi planning to introduce the system in high-security facilities, such as electric power plants and data centers (Insidethegames, 2016). Figure 15 presents security measures at venues.

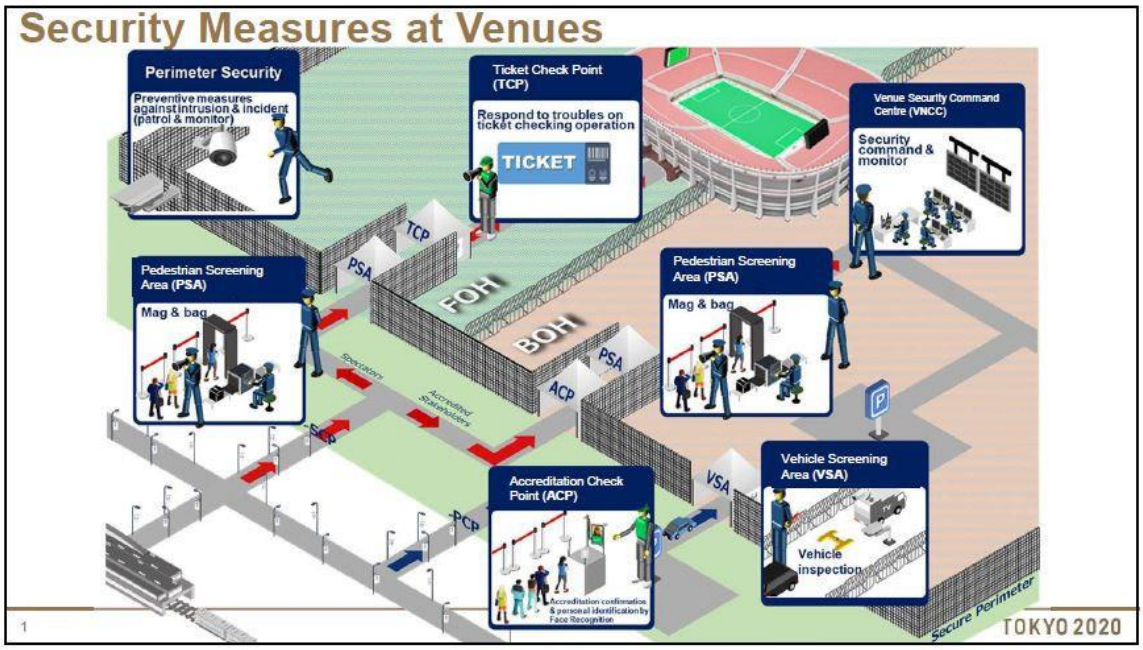


*Figure 15: Security measures at venues (O'Kane, 2019)*

Also, Tokyo 2021 became special due to the use of artificial intelligence (robots) to assist participants which is justified to observe also from a security perspective in terms of potential hacker threat.

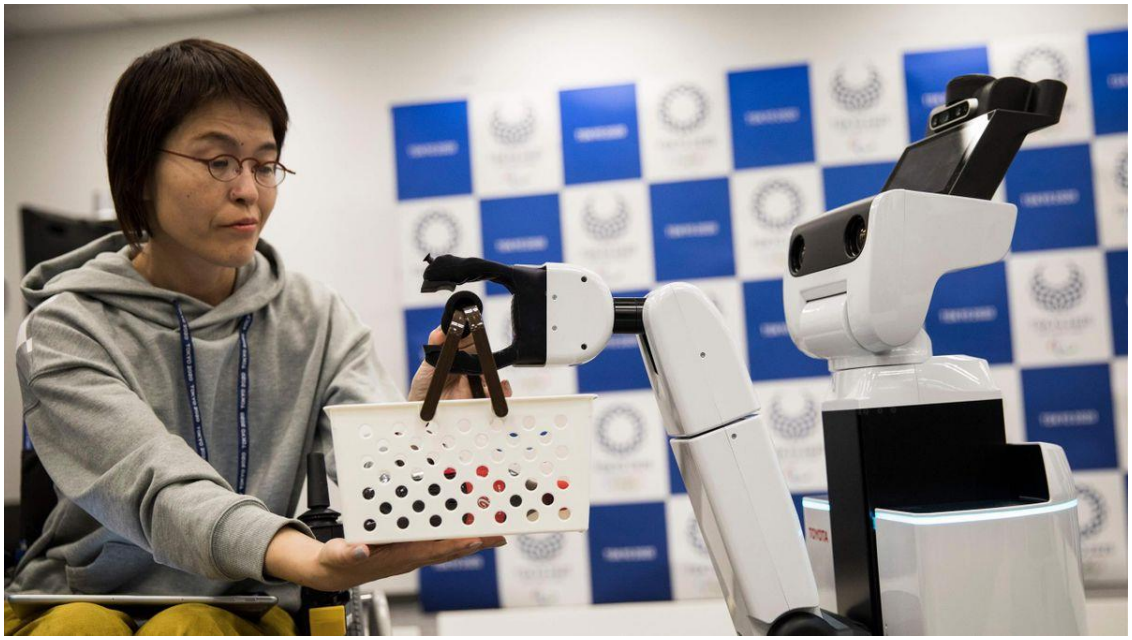

*Figure 16: Tokyo 2020 robot assistant (Reuters, 2019)*

Special attention is paid to the security of cyberspace. According to Dion-Schwarz et al. (2018) Japan's Cybersecurity Preparations for Tokyo 2020 Japan has established measures to protect critical national infrastructure in advance of Tokyo 2020, taking steps to harden cyber defenses and protect tourists and participants. Cybersecurity plans for Tokyo 2020 have been in development since at least 2015. Moreover, the Ministry of Internal Affairs and Communications requested approximately 181 million USD in funding for comprehensive cybersecurity measures in preparation for Tokyo 2020, highlighting the government's commitment to cybersecurity planning. The Japanese government committed to training 50 000 people in the public and private sectors specifically to guard the country against cyberattacks during Tokyo 2020 (Nikkei Asian Review, 2015). In 2017, a new training center for cybersecurity recruits was built in Tokyo to house a hands-

on cyber range, in anticipation of cyberattacks at the 2020 Olympics (Barker, 2017). In March 2017, the Japanese government held a large-scale cybersecurity drill to simulate an actual cyberattack involving the "world's largest" virtual network (Japan Times, 2017). Japan's cybersecurity planning efforts for Tokyo 2020 aimed to protect critical national infrastructure, harden cyber defenses, and protect tourists and participants. According to Dion-Schwarz et al. (2018), in responding to the changing cyber threat environment, the Cyber Security Strategic Headquarters has focused attention on the following initiatives and programs:

- A bot-cleansing campaign is aimed at comprehensively identifying affected and at-risk devices, disseminating updates and patches, and implementing an ongoing prevention campaign. Pending technical and legal issues must be resolved before internet service providers (ISPs) can assist with the bot-cleansing campaign.
- A new comprehensive information-sharing and collaborative network to promote collaboration among public-and private-sector stakeholders in an effort to contain cyberattacks from metastasizing into cascading system failures. The network is predicated on information-sharing agreements, which may require changes to relevant legislation.
- An Olympic-Paralympic CSIRT is planned to be established by March 2019 to assist the Tokyo 2020 Organising Committee on cybersecurity issues. The CSIRT is planned to consist of specially trained staff who will collaborate with external partners, service providers and security vendors.

- A security information center is planned to be stood up in the National Police Agency to support evidence collection, analysis, and evaluation of physical security incidents as they arise and to liaise with other relevant organizations.

Table 4 presents a prioritized Risk assessment of Tokyo Olympics based on a typology of hackers.

*Table 4: A prioritized Risk assessment of Tokyo Olympics based on a typology of hackers (Dion-Schwarz et al., 2018)*

| | | | Risk Analysis | | Risk Evaluation | |
|---|---|---|---|---|---|---|
| Threat Actor | Adversary Motivation | Sophistication | Likelihood | Impact | Prioritization | Rank |
| Foreign intelligence services | Ideology | High | Medium | High | High | 1 |
| Cyberterrorists | Ideology/revenge | Medium | Medium | High | Medium | 2 |
| Cybercriminals/ organized crime | Profit | High | Medium | Medium | Medium | 3 |
| Hacktivists | Ideology/revenge | Medium | Medium | Medium | Medium | 4 |
| Insider threats | Revenge/profit | Medium | Low | Medium | Medium | 5 |
| Ticket scalpers | Profit | Medium | High | Low | Low | 6 |

According to Dion-Schwarz et al. (2018) there are four high-level threat categories to prioritize in the run-up to Tokyo 2020:

1) Targeted attacks, aimed at high-profile Olympic assets, individuals, or organizations (e.g., broadcasting systems, Olympic commissioners, Japanese cybersecurity organizations), for either financial or political gain, could result in severe breaches or financial or reputational losses.
2) DDoS attacks against Tokyo 2020 infrastructure or associated networks could disrupt the availability of services or distract from other ongoing attacks. DDoS attacks could be launched by advanced threat actors, such as nation-states, or less

sophisticated groups, such as hacktivists. Particular attention should be paid to developments in DDoS methods, including IoT powered botnets.

3) Ransomware attacks could affect a wide range of devices, services, and underlying infrastructure supporting the Tokyo 2020 Olympics, including participant and visitor devices, transportation services, and point-of-sale systems.
4) Cyber propaganda or misinformation could be deployed to cause reputational loss for individuals, sponsor organizations, or the host nation. It could also be deployed for political purposes or to disrupt the Olympic Games themselves.

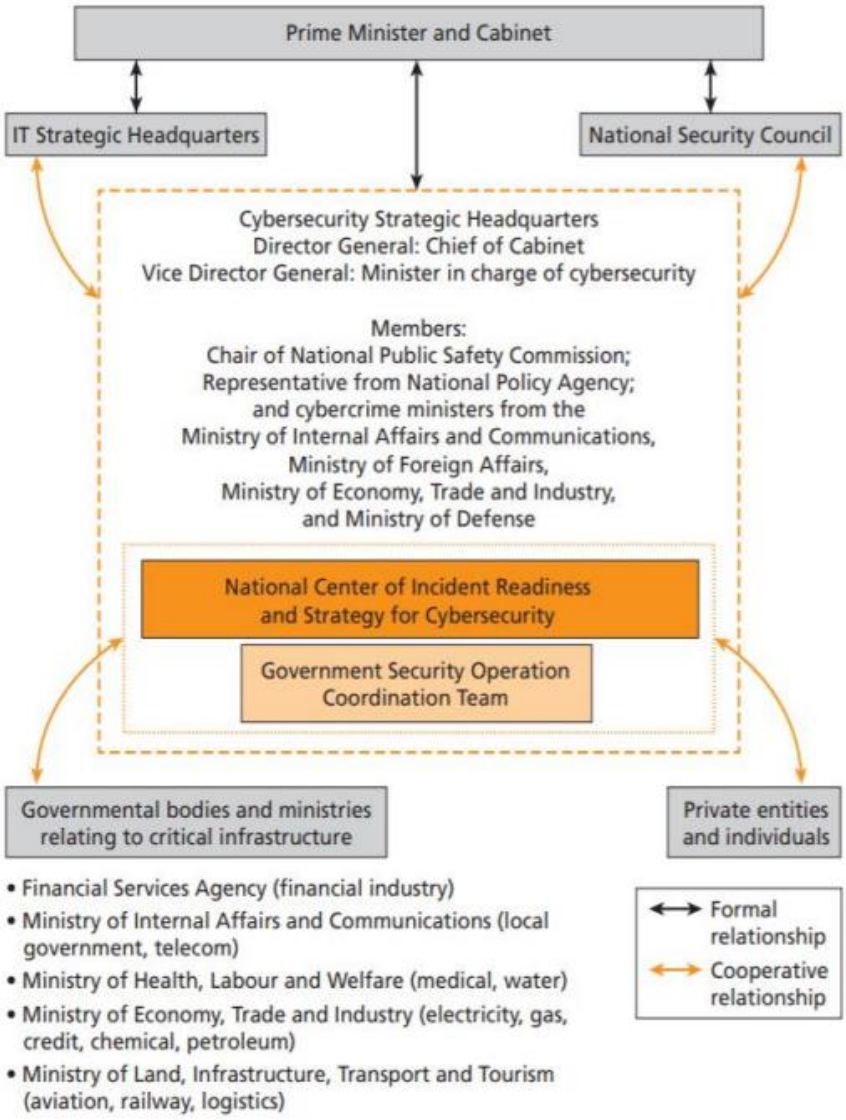


*Figure 17: Tokyo Olympics Cybersecurity Structure (Dion-Schwarz et al., 2018)*

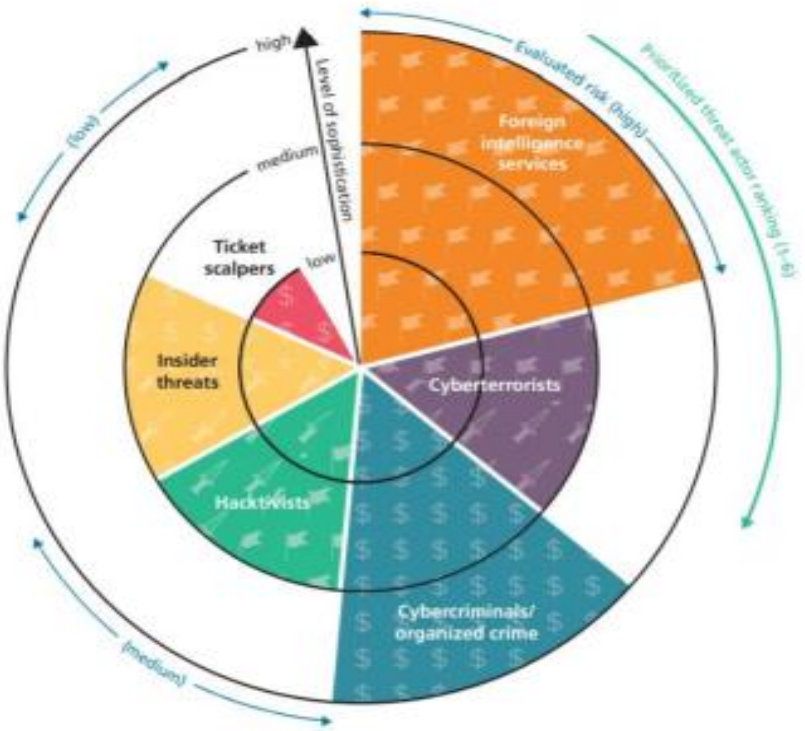


*Figure 18: Tokyo Olympics - Level of Threats (Dion-Schwarz et al., 2018)*

The global societal impact of the SARS-CoV-2 pandemic highlights the importance for Host Authorities of major sporting events to include crises and disaster contingency-planning in their preparations (United Nations Office of Counter-Terrorism, 2021). Ilevbare and McPherson (2022) even conceptualize the effects of SARS-CoV-2 as having connected similarities with the term hybrid threat. In security and safety context, additional effort had to be made into SARS-CoV-2-related issues, which included (The Tokyo Organizing Committee of the Olympic and Paralympic Games Update to the Sustainability Pre-Games Report, 2021):

- Avoidance of the 3Cs (Closed spaces, Crowded places, Close-contact settings);

- Prevention of infection spread by droplets and/or physical contact;
- Thorough disinfection;
- Comprehensive health management and checks;
- Detailed communication;
- Development of a response plan in cases where persons become infected or are suspected of being infected.

The Tokyo Games Organizing Committee initially estimated the security budget at about 900 million USD (Tokyo2020, 2019). Later on, another 900 million USD was estimated to be spent on measures to stop the spread of SARS-CoV-2. The games passed without a major security incident.

## 4.7 Comparative analysis and discussion

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

Horne and Manzenreiter (2006) have predicted that security issues are likely to come more to the fore in production of major sporting events and will form a substantial research theme in further studies of those events. 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, 2007). 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. Hence, the security costs exploded following the terror attacks in the United States, the United Kingdom and Spain in the 2000s.

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

The comparison of case studies shows the evolution of risks or their complication. 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. 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. The figure 19 presents a building-block approach to validation and test exercising.

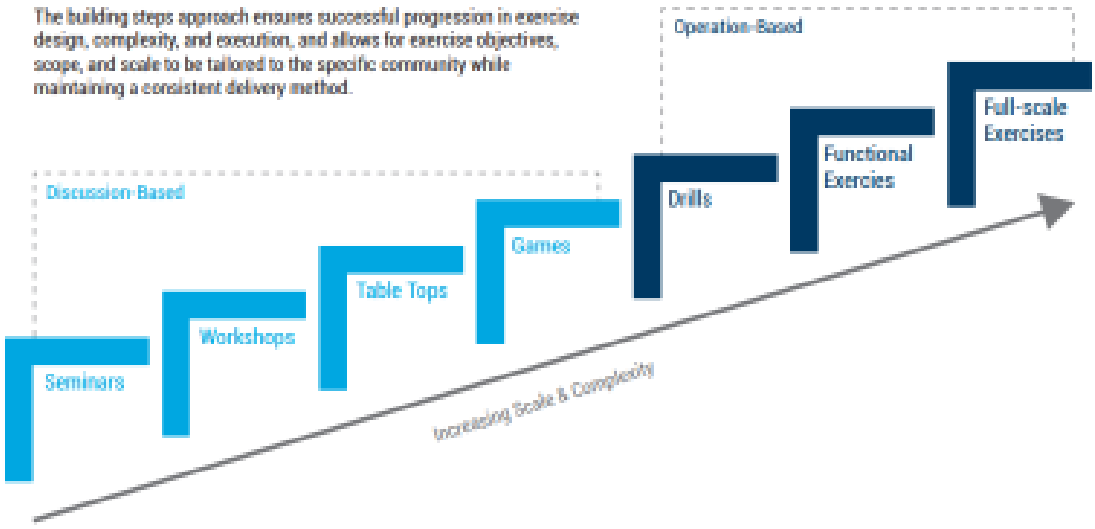


*Figure 19: A Building-Block Approach to Validation and Test Exercising. In: United Nations Office of Counter-Terrorism (2021): Guide on the security of major sporting events*

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.

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

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:

1) Sydney 2000: 250 million USD
2) Athens 2004: 1.5-1.6 billion USD
3) Beijing 2008: 6.5 billion USD
4) London 2012: 3.1 billion USD
5) 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)
6) 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 (Bennett and Haggerty, 2011). 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).

# CHAPTER V:

# FUTURE PERSPECTIVES

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

Looking to 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. The figure 20 presents the LA Security command structure.

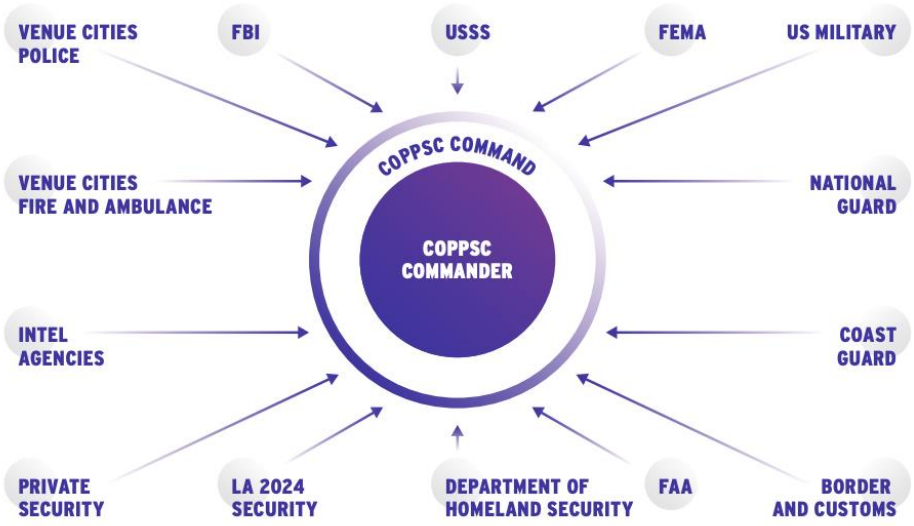


*Figure 20: Los Angeles Security command structure (LA 24/28 Bid book, Felker-Kantor, 2021)*

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 include 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.

# CHAPTER VI:

# 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. 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


Adelaide Now. 2017. *Sydney and Adelaide football fans clash outside Hindmarsh Stadium ahead of A-League match*. https://www.adelaidenow.com.au/news/south-australia/sydney-and-adelaide-football-fans-clash-outside-hindmarsh-stadium-ahead-of-aleague-match/news-story/1da3d17407d68640c4eb367b5747b42b (accessed March 15th 2022).

Alie, S.S. 2015. *Project governance: #1 critical success factor*. Paper presented at PMI® Global Congress 2015-North America, Orlando, FL. Newtown Square, PA: Project Management Institute.

Arquilla, J. & Ronfeldt, D. 2001. *The Advent of Netwar* (Revisited). In: Arquilla, J.; Ronfeldt, D. 2001. (ed.) Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: RAND.

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

Athanasidis, I. 2004. *Muslims Living in Greece Come Under Intelligence Spotlight Ahead of Olympics*. International Herald Tribune.

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*.

Baker, T. A.; Connaughton, D.; Zhang, J. J. & Spengler, J. O. 2007. *Perceived risk of terrorism and related risk management practices of NCAA Division IA Football Stadium Managers*. Journal of Legal Aspects of Sport 13, 2. 145-179.

Barbassa, J. 2017. *Safety for Whom? Securing Rio for the Olympics*. In: Rio 2016: Olympic Myths, Hard Realities, edited by Andrew Zimbalist, 153-178. Washington D.C.: Brookings.

Barker, S. 2017. *Japan Cybersecurity Skills Shortage in a 'State of Urgency' Before 2020 Olympics*, Security Brief Asia.

Bartoluci, M. & Škorić, S. 2008. *Ekonomski aspekti velikih sportskih priredbi, primjer Europskog nogometnog prvenstva*, Računovodstvo i financije, June, 182-187.

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

Bennett, C. & Haggerty, K.D. 2011. *Introduction to Security Games: Surveillance and Control at Mega-Events*. In: Security Games: Surveillance and Control at Mega-Events, eds C. Bennett and K.D. Haggerty, 1-19. Hoboken: Routledge.

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. & Mikulić, I. 2007. *Business intelligence i nacionalna sigurnost*. Polemos 10, 1. 27-43

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

Bilandžić, M. 2019. *Nacionalna sigurnost - prognoziranje ugroza*. Zagreb: Despot infinitus.

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

Boholm, M., Möller, N. & Hansson, S. O. 2015. *The concepts of risk, safety, and security: applications in everyday language*, Risk Analysis, 36, 3, 320-338.

Booz, A. & Cyber4Sight. 2016. *Rio Summer Olympic Games Cyberthreat Environment*, https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/white-paper/cyber4sight-special-report-rio-summer-olympics.pdf

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

Bourbeau, P.; Balzacq, T. & Cavelty, M. D. 2015. *International relations: Celebrating eclectic dynamism in security studies*. In: Bourbeau, P. 2015. (ed.) Security: Dialogue across Disciplines. Cambridge: Cambridge University Press.

Boyer, L., Musso, D., Barreau, G., Boyer Collas, L. & Addadi, A. 2007. *Organising a Major Sport Event*. In: J. Camy and L. Robinson (eds.) Managing Olympic Sport Organisations (pp. 279-343). Human Kinetics.

Boyle, P. & Haggerty, K. 2009. *Privacy Games: The Vancouver Olympics, Privacy and Surveillance*. Report to the Office of the Privacy Commissioner of Canada.

Boyle, P.J. & Haggerty, K.D. 2012. *Planning for the worst: Risk, uncertainty and the Olympic Games*. The British Journal of Sociology 63, 2, 241-59.

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.

Boyle, P.J. 2012. *Risk, Resiliency, and Urban Governance: The Case of the 2010 Winter Olympics*. Canadian Review of Sociology 49, 4, 350-69.

Brazilian Government. 2015. *Plano Estratégico de Segurança Integrada para os Jogos Olímpicos e Paralímpicos Rio 2016*. Diário Oficial da União - Portaria Interministerial No 1.678.

Brianas, J. 2004. *NATO, Greece and the 2004 Summer Olympics*. Naval Postgraduate School, Monterey, California. http://handle.dtic.mil/100.2/ADA429691

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.

Byman, D. 2014. *The Intelligence War on Terrorism. Intelligence & National Security*. Routledge: Taylor & Francis Group.

Cambridge Dictionary. 2019. *Sport*. https://dictionary.cambridge.org/dictionary/english/sport (accessed 20th March 2022)

Caspe, M. S. 1976. *An overview of project management and project management services*. Project Management Quarterly, 7, 4, 30-39.

Chaliand, G. & Blin, A. 2007. *Introduction*. In: Gerard Chaliand and Arnaud Blin (eds.), The History of Terrorism: From Antiquity to Al Qaeda (Berkeley: University of California Press), 1-11.

Chen, K., Feist, Z. &, Kapelke, C. 2017. *The Cybersecurity of Olympic Sports: New Opportunities, New Risks*, Betsy Cooper.

China Daily. 2005. available online at http://www.chinadaily.com.cn/english/doc/

Clarke, R. 2004. *Against all Enemies: Inside America's War on Terror*. New York: Free Press.

Clément, D. 2017. *The Transformation of Security Planning for the Olympics: The 1976 Montreal Games*. Terrorism and Political Violence 29, 1, 27–51.

Clemente, D. 2013. *Cybersecurity*. In: Dover, R.; Goodman, M. S.; Hillebrand, C. 2013. (ed.) Routledge Companion to Intelligence Studies. Routledge.

Coaffee, J., Fussey, P. & Moore, C. 2011. *Laminated Security for London 2012: Enhancing Security Infrastructures to Defend Mega Sporting Events*. Urban Studies 48, 15, 3311-27.

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

Connors, E. 2007. *Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement*. Institute for Law and Justice, Alexandria, Virginia. Prepared for the Office of Community Oriented Policing Services, U.S. Department of Justice, Washington, D.C.

Council of Europe. 2019. *The Committee on Safety and Security at Sports Events*.

Crelier, A. 2019. *Trend Analysis Cybersecurity at Big Events*. Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich, Retrieved from: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securitiesstudies/pdfs/Cyber-Reports-2019-11-Cybersecurity-at-Big-Events.pdf.

Croft, S. 2008. *What Future for Security Studies?* In: Williams, P. D. 2008. (ed.) London and New York: Routledge. Taylor & Francis Group.

Cronin, K. A. 2009. *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*. Princeton and Oxford: Princeton University Press.

Cunningham, G. 2007. *Security management capabilities in intercollegiate athletic departments*. Unpublished doctoral dissertation. The University of Southern Mississippi.

Čustonja, Z. & Škorić, S. 2011. *Winning medals at the Olympic Games - does Croatia have any chance?* Kinesiology, 43, 1, 107-114.

De Bosscher, V. 2016. *A mixed methods approach to compare elite sport policies of nations. A critical reflection on the use of composite indicators in the SPLISS study* /online/. Sport in Society.

Decker, S.H., Greene, J.R., Webb, V., Rojeck, J., McDevitt, J., Bynum, T., Varano, S. & Manning., P.K. 2005. *Safety and Security at Special Events: The Case of the Salt Lake City Olympic Games*. Security Journal, 18, 4.

Desiderá, L. 2016. *CERT.br, Lessons Learned from the Rio2016 Summer Olympic Games*. Presentation at the San José FIRST Technical Colloquium, San José, Costa Rica.

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.

Duckworth, A. & Hunt, T.M. 2016. *Protecting the Games. The International Olympic Committee and Security, 1972-1984*. Olympika 25, 1, 67-87.

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

Felker-Kantor, M. 2021. *Op-Ed: Hosting the Olympics Will Only Increase Mass Surveillance and Policing in Los Angeles*. https://knock-la.com/los-angeles-olympics-city-council-coppsc-policing/ (accessed 15th March 2022).

Foucault, M. 1991. *Politics and the study of discourse*. In: Burchell, G.; Gordon, C.; Miller, P. 1991. (ed.) The Foucault Effect: Studies in Governmentality. University of Chicago Press.

Frazier, D. & Stewart-Ingersol, R. 2010. *Regional powers and security: A framework for understanding order within regional security complexes*. European Journal of International Relations 16, 4, 731-753.

Freeman, J. & Burgos, M. 2017. *Accumulation by Forced Removal: The Thinning of Rio de Janeiro's Favelas in Preparation for the Games*. Journal of Latin American Studies 49, 3, 349-77.

Friedman, A. 2003. *Terrorism in Context*. In: Terrorism: Concepts, Causes and Conflict Resolution. Advanced Systems and Concepts Office, Defense Threat Reduction Agency and Working Group on War, Violence and Terrorism. Institute for Conflict Analysis and Resolution, George Mason University. Fort Belvoir, Virginia.

Furedi, F. 2009. *Poziv na teror: Rastuće carstvo nepoznatog*. Zagreb: Naklada Ljevak.

Fussey et al. 2001. *Securing and Sustaining the Olympic City*; Colin Bennett and Kevin Haggerty (eds), Security Games: Surveillance and Control at Mega-Events (London: Routledge).

Fussey, P. & J. Coaffee 2012a. *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.

Fussey, P. & J. Coaffee. 2012b. *Olympic rings of steel: Constructing security for 2012 and beyond*. In: Security Games: Surveillance and Control at Mega-Events, eds C. Bennett and K.D. Haggerty, 36-54. Hoboken: Routledge.

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

Fussey, P. 2015. *Command, control and contestation: negotiating security at the London 2012 Olympics*. The Geographical Journal 181, 3, 212-23.

Gaffney, C. 2016. *The Brazilian experience as role model*. In: Sweeney, G.; McCarthy, K. 2016. (ed.) Global Corruption Report: Sport. Transparency International. Routledge

Gerecht, M. R. 2001. *The Counterterrorist Myth.* http://www.theatlantic.com/past/docs/issues/2001/07/gerecht.htm (accessed March 1st 2022)

Gerges, F. A. 2011. *The Rise and Fall of Al-Qaeda*. Oxford University Press.

Getz, D. 1997. *Event Management and Tourism*. New York: Cognizant.

Giulianotti, R. & Klauser, F. 2010. *Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda*. Journal of Sport and Social Issues 34, 1, 48-60.

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

Glass, R. R. & Davidson, P. B. 1948. *Intelligence is for Commanders*. Harrisburg, PA., Military Service Pub.

Goud, N. 2018. *No Cyber Attacks on FIFA World Cup 2018*, Retrieved from: https://www.cybersecurity-insiders.com/no-cyber-attacks-on-fifa-world-cup-2018

Greenwell, T.C., Danzey-Bussell, L.A. & Shonk, D.J. 2014. *Managing sport events*. Human Kinetics.

Gregory, S. 2016. *Terror Threat Looms as Olympians Ready to Compete in Rio*. Time, August 5, 2016. http://time.com/4438690/rio-2016-olympics-terrorism-security/.

Guardian. 2016. *Brazil lends $895m to Rio de Janeiro's security fund for Olympics*. https://www.theguardian.com/world/2016/jun/30/brazil-rio-de-janeiro-olympics-loan-security-subway

Gunaratna, R. & Oreg, A. 2010. *Al Qaeda's Organizational Structure and its Evolution*. Studies in Conflict & Terrorism 33, 12, 1043-1078.

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

Hall, S. 2006. *Effective security management of university sports venues*. The Sport Journal 9/4.

Hassan, D. 2012. *Sport and terrorism: Two of modern life's most prevalent themes*. International Review for the Sociology of Sport 47, 3, 263-267.

Herring, P. J. 2005. *Create an Intelligence Program for Current and Future Business Needs*. Competitive Intelligence Magazine. 8, 5, 20-27.

Hoare, O. 2018. *London 2012: Cyber Security, presentation slides, undated*. UK Home Office. https://www.ipa.go.jp/files/000037535.pdf

Home Office. 2011a. *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)

Home Office. 2011b. *Contest*. UK Government, London. http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat/ (accessed 30th March 2022)

Hopkins, N. & R. Booth. 2012. *Olympic security chaos: Depth of G4S security crisis revealed*. The Guardian, London. http://www.guardian.co.uk/sport/2012/jul/12/london-2012-g4s-security-crisis

Horne, J. & Manzenreiter, W. 2006. *An Introduction to the Sociology of Sports Mega Events*. Sociological Review 54, 2, 19.

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.

Houston Chronicle. 2007. *Olympic security expert: terrorist attack on sports event 'just a matter of time'*.

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.

Insidethegames. 2016. *Japan develop security technology in bid to tackle terrorism threat at Tokyo 2020*. https://www.insidethegames.biz/articles/1042471/japan-develop-security-technology-in-bid-to-tackle-terrorism-threat-at-tokyo-2020

International Institute for Counter-Terrorism. 2000. *Olympic Bomb Plot to Blow up Sydney Nuclear Reactor Foiled: How Serious the Threat*. https://www.ict.org.il/Article.aspx?ID=786#gsc.tab=0 (Accessed March 27th 2022).

Intriligator, M. D. 2010. *The Economics of Terrorism*. Economic Inquiry 48, 1, 1-13.

IOBE (Foundation for Economic & Industrial Research). 2015. *The impact of the 2004 Olympic Games on the Greek economy, Athens*.

IOC 1992. *Minutes of the 98th Session of the International Olympic Committee*, held in Courchevel, February 5 and 6, 1992. Lausanne. IOC Archive.

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.

Jago, L. & Shaw, R. 1998. *Special events: a conceptual and differential framework*. Festival Management and Event Tourism, 5, 1/2, 21-32.

Japan Times. 2017. *Government to Hold Massive Anti-Cyberattack Drill for 2020 Tokyo Olympics*.

Jennings, W. 2012. *Olympic Risks*. London: Palgrave.

Johnson, C. 2008. *Using Evacuation Simulations to Ensure the Safety and Security of the 2012 Olympic Venues*. Safety Science, 302-322.

Jones, S. G. & Libicki, M. C. 2008. *How Terrorist Groups End: Lessons for Countering al Qa'ida*. Santa Monica: RAND Corporation.

Jore, S. H. 2019. *The Conceptual and Scientific Demarcation of Security in Contrast to Safety*. European Journal of Security Resources, 4, 2, 157-174.

Jore, S.H. & Egeli, A. 2015. *Risk management methodology for protecting against malicious acts? Are probabilities adequate means for describing terrorism and other security risks?* In: Podofillini, L., Sudret, B., Stojadinovic, B., Zio, E. and Kröger, W. (eds.) Safety and Reliability of Complex Engineered Systems, London: CRC Press, 807-815.

Kao, J. S. 2016. *The cost of building the 2016 Rio Olympics*. Financial Times. Retrieved 30th March 2022 from https://www.f.com/content/52ce2456-5b71-11e6-9f70-badea1b336d4.

Kennelly, M. 2005. *Business as usual: Elite Australian athletes' viewpoints of terrorism post 9/11*. Unpublished honours thesis, University of Technology, Sydney.

Khalifa, N.K.A.A-D. 2020. *Identification and Prevention of Expected Cybersecurity Threats During 2022 FIFA World Cup in Qatar*. Journal of Poverty, Investment and Development 5, 1-4, 49-84.

King, N. 2016. *Sport, Terrorism, National Security, and the Deep State: Components of a Longitudinal Research Programme*. In: Harvey, A.; Kimball, R. 2016. (ed.) Sport: Identity and Community. Oxford: Inter-Disciplinary Press.

Kirkpatrick, B. L. 1997. *Intelligence*. In: Jentelson, W. B. & Paterson, G. T (eds.) Encyclopedia of US Foreign Relations, Volume 2. New York, Oxford University Press

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.

Lawson, C. 1985. *Intergovernmental Challenges of the 1984 Olympic Games*. Publius, 127-141.

Lechner, F.M. 2014. *Security threats to the Olympic Games*. Master's Thesis. University of Peloponnese.

Lenskyj, H.J. 2002. *The Best Olympics Ever? The Social Impacts of Sydney 2000*. Albany: Suny Press.

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.

Leško, L. 2019. *Analitičke tehnike primjenjive u sigurnosno-obavještajnim agencijama. [Analytical techniques applicable in the Intelligence Agencies]*, Strategos, 3, 2, 7-35.

Loader, I. & Walker, N. 2007. *Civilizing security*. New York: Cambridge University Press.

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.

Lynch, R. & Cuccia, P. 2006. *NATO: Rewarding service in the alliance*. Military Review, January-February: 54-58.

Lyon, D. & Murakami Wood, D. 2012. *Security, Surveillance, and Sociological Analysis*. Canadian Review of Sociology 49, 4, 317-27.

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

Malik, S. 2015. *Constructing security*. In: Hough, P. et al. 2015. (ed.) International Security Studies: Theory and Practice. New York - Abingdon: Routledge.

Marketplace. 2016. *Let's do the numbers: The money spent on the Rio Olympics*. https://www.marketplace.org/2016/08/05/let-s-do-numbers-what-has-been-spent-rio-olympics/

Martel, F. 2015. *Report: ISIS Recruiting 'Lone Wolf' Jihadists in Brazil to Attack 2016 Olympics*. Breitbart, March 23, 2015, at http://www.breitbart.com/national-security/2015/03/23/report-isis-recruiting-lone-wolf-jihadists-inbrazil-to-attack-2016-olympics/

Masterman, G. 2004. *Strategic Sports Events Management. An International Approach*. http://www.pseudology.org/TerOvanesian/Masterman_Strategic_Sports_Event_Management2.pdf

Matheson, V. 2013. *Assessing the infrastructure impact of mega-events in emerging economies*. In: Infrastructure and Land Policies, Gregory K. Ingram and Karin L. Brandt, eds., (Cambridge, MA: Lincoln Land Institute, 2013), 215-232.

Mcdonald, M. 2008. *Constructivism*. In: Williams, P. D. 2008. (ed.) Security Studies: An Introduction. London and New York: Routledge, Taylor & Francis Group.

Merriam-Webster. 2022. *Governance*. https://www.merriam-webster.com/dictionary/governance (accessed 28th March 2022).

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*.

MIT Technology Review. 2019. *Russian hackers are infiltrating companies via the office printer*. https://www.technologyreview.com/f/614062/russian-hackers-fancy-bear-strontium-infiltrate-iot-networks-microsoft-report/ (accessed 30th March 2022).

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

NaCTSO. 2014. *Counter Terrorism Protective Security Advice for Stadia and Arenas*.

National Audit Office. 2012. *The London 2012 Olympic Games and Paralympic Games: post-Games review*. Report by the comptroller and Auditor general. HC 794. London.

Neumann, B. I. 2010. *National security, culture and identity*. In: Dunn Cavelty, M.; Mauer, V. 2010. (ed.) The Routledge Handbook of Security Studies. Abingdon/New York: Routledge Taylor & Francis Group.

Nikkei Asian Review. 2015. *Japan to Deepen Ranks of Network Defenders with Eye to Olympics*.

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).

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Oxford, UK: Berg.

NPR. 2008. *Mexico's 1968 Massacre: What Really Happened?* https://www.npr.org/templates/story/story.php?storyId=97546687 &t=1568790149378 (accessed March 15th 2022).

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

Organizing Committee of the 1976 Montreal Olympic Games. 1978. *Games of the XXI Olympiad, Montreal 1976: Official Report, Volume 2*. Montreal: Organizing Committee of the 1976 Montreal Olympic Games.

Ormsby, A. 2010. *London Olympics 'unavoidably attractive' for cyber-attacks.* http://uk.reuters.com/article/idUKTRE6AO2QY20101125 (accessed March 14th 2022).

O'Kane, P. 2019. *Face recognition among security checks planned for Tokyo 2020 venues*. https://www.insidethegames.biz/articles/1085983/security-chief-outlines-spectator-checks (accessed 15th March 2022).

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.

Panetta, L. & Newton, J. 2014. *Worthy Fights: A Memoir of Leadership in War and Peace*. USA: Penguin Publishing Group.

Parent, M.M. 2015. *Chapter 3: The Organizing Committee's Perspective*. In: M.M. Parent, J-L. Chappelet, Routledge Handbook of Sports Event Management, 43-64.

Pennell, G. 2013. *Speaking at a cybersecurity event*.

Phythian, M. 2014. *Understanding the Intelligence Cycle*. London/New York, Routledge, Taylor and Francis Group.

Pillar, P. R. 2011. *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform*. Columbia University Press.

Pizam, A. & Smith, G. 2000. *Tourism and Terrorism: A Quantitative Analysis of Major Terrorist Acts and Their Impact on Tourism Destinations*. Tourism Economics 6, 2, 123-138.

Plecas, D., Dow, M., Diplock, J. & Martin, J. 2010. *The Planning and Execution of Security for the 2010 Winter Olympic Games 38 Best Practices and Lessons Learned*. University of the Fraser Valley & Centre for criminal justice research.

PMI (Project Management Institute). 2000. *A Guide to the Project Management Body of Knowledge*. http://www. cs.bilkent.edu.tr/~cagatay/cs413/PMBOK.pdf Retrieved in March 2022.

Portland's In-house Content & Brand Team. 2018. *The Soft Power 30. A Global Ranking of Soft Power*.

Preuss, H. 2015. *A framework for identifying the legacies of a mega sport event* /online/. Leisure Studies, 34, 6.

Preuss, H., Andreff, W. & Weitzmann, M. 2019. *Cost and Revenue Overruns of the Olympic Games 2000-2018*. Springer Gabler.

Promotion Film for the Security of Beijing Olympics. 2007.

Randall, A. 2008. *21st-century security and CPTED,* Boca Raton, Florida: CRS Press.

Reniers, G. L. & Audenaert, A. 2014. *Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures with domino effects*. Process Safety and Environment Protection, 92(6), 583-589.

Reniers, G. L., Cremer, K. & Buytaert, J. 2011. *Continuously and simultaneously optimising an organisation's safety and security culture and climate: the improvement diamond for excellence achievement and leadership in safety and security (IDEAL SandS) model*. Journal of Clean Production, 19, 11, 1239-1249.

Reuters. 2016. *ISIS's Latest Threat?* http://english.alarabiya.net/en/perspective/features/2016/04/16/Brazil-sees-rising-threat-from-ISIS-says-intelligenceagency.html

Reuters. 2019. *Olympics News - Tokyo 2020 Unveils Robots to Help Wheelchair Users.* https://www.eurosport.co.uk/olympics/tokyo-2020/2021/olympics-news-tokyo-2020-unveils-robots-to-help-wheelchair-users_sto7186981/story.shtml

Richards, A., Fussey, P. & Silke, A. 2011. *Terrorism and the Olympics: Major event security and lessons for the future*. London: Routledge.

Riding, A. 1992. *Olympics; Keeping Terrorism at Bay in Barcelona*. New York Times, July 21, 1992. https://www.nytimes.com/1992/07/11/sports/olympics-keeping-terrorism-at-bay-inbarcelona.html.

Risley, S. 2006. *The Sociology of Security: Sociological Approaches to Contemporary and Historical Securitization*. The annual meeting of the American Sociological Association. Montreal: Montreal Convention Center.

Rodrigues, A. 2016. *Brazilian Intelligence Agency Confirms Terrorist Message Against the Country*. Agência Brasil, http://agenciabrasil.ebc.com.br/en/geral/noticia/2016-04/brazilian-intelligence-agency-confirmsterrorist-message-against-country.

Rogerson, J.R. 2016. *Re-defining temporal notions of event legacy: lessons from Glasgow's Commonwealth Games*. Annals of Leisure Research, 19, 4, 497-518.

Samatas, M. 2004. *Surveillance in Greece: From anticommunist to the consumer surveillance*. New York: Pella.

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.

Schmid, A. P. 2004. *Terrorism - The Definitional Problem*. Case Western Reserve Journal of International Law 36, 2-3. 375-419.

Schmid, A. P. 2011. *The Routledge Handbook of Terrorism Research*. London/New York: Routledge.

Scott, H. 2009. *Governance of Terror: New Institutionalism and the Evolution of Terrorist Organizations*. Public Administration Review 69, 4, 727-739.

Security Command Centre for the Games of XXIX Olympiad. 2007. http://www.bjayab.cn/webapp/ayabweb/english/subindex.do?ck¼CATE1_ENG_ABDT&ai¼ 10453, accessed 15th March 2022.

Security Industry Association. 2007. *China Security Market Report Special Supplement: Olympic Update*. Alexandria, Virginia: Security Industry Association.

Sen, A. 2007. *Identitet i nasilje: Iluzija sudbine*. Zagreb: Poslovni dnevnik, Masmedia.

Shiraz, Z. & Aldrich, R. J. 2013. *Globalisation and Borders*. In: Dover, R.; Goodman, M. S.; Hillebrand, C. 2013. (ed.) Routledge Companion to Intelligence Studies. Routledge.

Siemens. 2007. *Major Event Security Solutions*. Online presentation. https://ppt-online.org/558065

Škorić, S., Aliti, B. & Leško, L. 2017. *Distribution Of Workforce Through Project Life Cycles and Analysis of The Satisfaction with The Organisation*. In: 8th International Scientific Conference on Kinesiology (eds.: Milanović, D., Sporiš, G., Šalaj, S. and Škegro, D.) 481-484.

Smartsheet. 2022. *Demystifying the 5 Phases of Project Management*. https://www.smartsheet.com/blog/demystifying-5-phases-project-management

Social Communication Secretariat (International Area Office of the President of Brazil). 2016. *Security in the Rio 2016 Olympic and Paralympic Games*. Brasilia. (Accessed 30th March 2022) from http://www.brasil2016.gov.br/en/presskit/fles/fact-sheet-security

Soliyev, N. 2014. *Terrorist threat to Sochi Olympics: testing time for Russia*. Nanyang Technological University, Singapore. (Accessed 30th March 2022), from http://hdl.handle.net/10220/19903.

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.

Stampnitzky, L. 2013. *Disciplining Terror: How Experts Invented 'terrorism'*. Cambridge/New York: Cambridge University Press.

Suburban Emergency Management Project (SEMP). 2005. *Securing the 1996 Centennial Olympic Games in Atlanta: Parts I and II*. http://www.semp.us/publications/biotID=205 (accessed 20th March 2022).

Sudworth, J. 2006. *Slum dispute over Commonwealth Games*. http://news.bbc.co.uk/1/hi/world/south_asia/5325034.stm (accessed March 16th 2022).

Sugden, J. 2012. *Watched by the Games: Surveillance and Security at the Olympics*. In: Watching the Olympics. Politics, Power and Representation, edited by Alan Tomlinson and John Sugden, 228-241. London: Routledge.

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.

Šušnjara, D. 2017. *Politika straha i terorizam: komparativna analiza protuterorističkih strategija Europske unije i Sjedinjenih Američkih Država*. Polemos 20, 39-40. 147-166.

Tennismash. 2016. *Nadal hit by Fancy Bear leak*. https://tennismash.com/2016/09/20/nadal-hit-fancy-bear-leak/ (Accessed 30th March 2022).

The Al Qaeda Manual. 2000. *Declaration of jihad [holy war] against the country's tyrants military series*. https://fas.org/irp/world/para/aqmanual.pdf (Accessed March 14th 2022).

The Anholt-gfk Roper Nation Brands Index. 2009. *GfK Roper Public Affairs & Media*. Prepared for Switzerland.

The First. 2005. (in Chinese) http://www.bj.xinhuanet.com/bjpd_tpk/2005-03/10/content_3847801.htm

The Star. 2017. *Canadian athletes, athletic organizations targeted by Russian hackers*. https://www.thestar.com/news/world/2017/02/23/canadian-athletes-athletic-organizations-targeted-by-russian-hackers.html (Accessed 30th March 2022)

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

The White House. 2018. *National Strategy for Counterterrorism of the United States of America*. The White House. Washington, DC.

Thompson, D. 2008. *Olympic security collaboration*. China Security Review, 4, 2, 46-58.

Toohey, K. & Taylor, T. 2012. *Surveillance and securitization: A forgotten Sydney Olympic legacy*. International Review for the Sociology of Sport 47, 3, 324-37.

Toohey, K. & Taylor, T. 2008. *Mega Events, Fear and Risk: Terrorism at the Olympic Games*. Journal of Sports Management, 451-469.

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.

Tosini, D. 2007. *Sociology of Terrorism and Counterterrorism: A Social Science Understanding of Terrorist*. Sociology Compass 1, 2, 664–681.

TrendMicro. 2018. *Sporting Event Threats: Lessons from the 2018 FIFA World Cup*. Retrieved from: https://www.trendmicro.com/vinfo/se/security/news/cybercrime-and-digitalthreats/sporting-event-threats-lessons-from-the-2018-fifa-world-cup.

Tulloch, J. 2000. *Terrorism, "Killing Events," and their Audience: Fear and Crime at the 2000 Olympics*. In: Kay Schaffer and Sidonie Smith (eds), The Olympics at the Millennium: Power, Politics and the Games (New Brunswick, NJ: Rutgers University Press, 2000), 224-40.

United Nations Office of Counter-Terrorism. 2021. *Guide on the security of major sporting events.*

United Nations. 2005. *Sport as a Tool for Development and Peace: Towards Achieving the United Nations Millennium Development Goals*.

Van Munster, R. 2005. *Logics of Security: The Copenhagen School, Risk Management and the War on Terror*. Political Science Publications. Faculty of Social Sciences. University of Southern Denmark.

Visacro, A. 2017. *Brazilian Organization for Combating Terrorism during the Rio 2016 Olympic Games and Paralympic Games*. Military Review September-October 2017, 94-104.

Voulgarakis, G.V. 2005. *Securing the Olympic Games: A model of international cooperation to confront new threats*. Mediterranean Quarterly 16, 4, 1-7.

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

Wæver, O. 2011. *Politics, security, theory*. Security Dialogue 42, 4-5. 465-480.

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

Wasterbeek, H.M., Turner, P. & Ingerson, L. 2002. *Key success factors in bidding for hallmark sporting events*. International Marketing Review, 19, 3, 303-322.

Weiss, M. & Hassan, H. 2015. *ISIS: u srcu vojske terora*. Zagreb: Buybook.

Whelan, C. 2012. *Networks and National Security: Dynamics, Effectiveness and Organisation*. Aldershot: Ashgate.

Whelan, C. 2014. *Surveillance, Security and Sports Mega Events: Toward a Research Agenda on the Organisation of Security Networks*. Surveillance & Society 11, 4, 392-404.

Wilson, S. 2004. *IOC close to deal for cancellation insurance*. http://slam.canoe.ca/Slam/Olympics/2004Athens/2004/04/19/428832-ap.html (Accessed March 15th 2022)

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

Wolfers, A. 1962. *National security as an ambiguous symbol*. Political Science Quarterly, 67, 4, 481-502.

Woodward, J.D. 2001. *Super Bowl Surveillance - Facing Up to Biometrics*. RAND Arroyo Center.

World Economic Forum. 2016. *The cost of hosting every Olympics since 1964*. Joe Myers: https://www.weforum.org/agenda/2016/07/the-cost-to-cities-of-hosting-the-olympics-since-1964/ (Accessed 15th March 2022).

World Health Organization. 2006. *Steps for Health: A European framework to promote physical activity for Health*.

Xing, X. & Chalip, L. 2012. *Challenges, obligations, and pending career interruptions: securing meanings at the exit stage of sport mega-event work*. European Sport Management Quarterly, 12, 4, 375-396.

Xinhua News. 2005. Available online at http://news.sports.cn/others/others/2005-03-25/519183.html.

Xinhua News. 2007. (in Chinese) http://news.xinhuanet.com/sports/2007-04/04/

Xinhua News. 2007. (in Chinese) http://www.hainan.gov.cn/data/news/2007/09/ 37786/ (in Chinese).

Yan, H., Jones, J. & Darlington, S. 2016. *Brazilian police arrest 12 suspected of planning terrorist acts during Olympics*. CNN, July 25, 2016. https://edition.cnn.com/2016/07/21/americas/brazil-olympics-terror-arrests/index.html.

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.

Zhang, D. & Zhang, H. 2008. *Troop Deployment for Olympic Security Has Been Completed; Armed Police Force Holds Olympic Security Expedition and Oath-Taking Rally; Meng Jianzhu and Other Attend and Speak*. Xinhua.