UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

unicri

UNAOC

ICSS
Safeguarding Sport

# GUIDE ON THE SECURITY OF MAJOR SPORTING EVENTS

## PROMOTING SUSTAINABLE SECURITY AND LEGACIES

SPORTS

countries
preparations
effective
including
Establish
resources
assessments
involved
provide
organisations
stage
governance
support
Chapter
event
Design
process
agencies
venues
local
MSE
infrastructure
Ensure
law
Develop
costs
Set
communication
operations
approach
civil
planning
sharing
strategy
protection
time
levels
stakeholders
security
security-related
measures
international
management
public
acts
enforcement
information
private
legal
Engagement

# Table of Contents

# Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies

*Within the framework of the United Nations Global Programme on the Security of Major Sporting Events and the Promotion of Sport and its Values as a Tool to Prevent Violent Extremism*

co-implemented by the
United Nations Office of Counter-Terrorism (UNOCT), in association with the United Nations Interregional Crime and Justice Research Institute (UNICRI), the United Nations Alliance of Civilizations (UNAOC) and the International Centre for Sport Security (ICSS)

in consultation with the Counter-Terrorism Committee Executive Directorate (CTED)

## ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AAR | After Action Report |
| AFRIPOL | African Police Cooperation Organisation |
| AIMC | Arab Interior Ministers’ Council |
| AMERIPOL | Police Community of the Americas |
| API | advance passenger information |
| ASEANAPOL | Inter-ASEAN Police |
| C2ConOps | Command and Control Concept of Operations |
| CAF | Confederation of African Football |
| CAGR | compound annual growth rate |
| CAZ | Controlled Access Zone |
| CBC | Cross Border Cooperation |
| CBM | Coordinated Border Management |
| CBRN | chemical, biological, radiological, nuclear |
| CoE | Council of Europe |
| COJO | Organizing Committee of the Olympic Games [Paris, 2024] |
| CONMEBOL | Confederación Sudamericana de Fútbol |
| CRG | community relations group |
| DDS | Drone Denial System |
| DDoS | Distributed Denial-of-Service |
| DPF | Data Protection Framework |
| EMS | Emergency Management System |
| Eurojust | European Union Agency for Criminal Justice Cooperation |
| EUROPOL | European Union Agency for Law Enforcement Cooperation |
| EVD | Ebola virus disease |
| FIFA™ | Fédération Internationale de Football Association |
| Fire-EMS | Fire-Emergency Medical Service |
| GCCPOL | General Secretariat of the Cooperation Council for the Arab States of the Gulf |
| GIS | Geographical Information System |
| IAEA | International Atomic Energy Agency |
| ICC | International Cricket Council |

| | |
|---|---|
| ICSS | International Centre for Sport Security |
| IBIS | Integrity Betting Intelligence System |
| IMEST | INTERPOL Major Event Support Team |
| IMIT | information management information technology |
| INTERPOL | International Criminal Police Organization |
| IOC | International Olympic Committee |
| ISAO | Information Sharing and Analysis Organizations |
| ISCT | Integrated Security Communication Team |
| ISF | international sport federation |
| ISO | International Organization for Standardization |
| ISU | Integrated Security Unit |
| IZ | Interdiction Zone |
| JOPG | Joint Operational Planning Group |
| LGBTQIA+ | Lesbian, gay, bisexual, transgender, queer (or questioning), intersex, asexual + |
| LOC | Local Organizing Committee |
| MSE | major sporting event |
| OECD | Organization for Economic Co-operation and Development |
| OSAC | Overseas Security Advisory Council (US State Department) |
| OSCE | Organization for Security and Cooperation in Europe |
| PNR | Passenger Name Records |
| PPP | Public-Private Partnership |
| PSA | Pedestrian Screening Area |
| PWGSC | Public Works and Government Services Canada |
| RAM | Responsibility and Accountability Matrix |
| RAZ | Restricted Access Zone |
| SET | Senior Executive Team |
| SKMS | Project Stadia Knowledge Management System |
| SoPs | Standard Operating Procedures |
| TRA | Threat Risk Assessments |
| UEFA | Union of European Football Associations |
| UNOCT | United Nations Office of Counter-Terrorism |
| UNSDGs | United Nations Sustainable Development Goals |

| | |
|---|---|
| UNTOC | United Nations Convention against Transnational Organized Crime |
| VANOC | Vancouver Organizing Committee |
| VSA | Vehicle Screening Area |
| WHO | World Health Organization |

## FOREWORD

In 2020, the United Nations marked its 75th anniversary. The values enshrined in the Charter of the United Nations in 1945 aimed to make the world a better place for all. It is with the same spirit that the General Assembly passed resolution 71/291 in 2017, establishing the United Nations Office of Counter-Terrorism (UNOCT) and recognizing the importance of countering terrorism and preventing violent extremism. In these endeavours to make the world a better place and to counter and prevent terrorism and violent extremism, there are few allies as powerful as sport and its values.

Historically, terrorist groups attempted, and continue, to strike sporting events. They are not solely targeted because they are attended by large groups of people, but also because they represent what terrorists aim to destroy in our societies and across the world. Sport is an extraordinary generator of positive values and an unparalleled unifying power, which can transcend civilizational and cultural barriers. Sport and sporting events play a significant role in addressing and preventing violent extremism by promoting the empowerment of youth and women and by facilitating integration. Sport pushes people to be better, to aim higher and further. It promotes tolerance and gender equality, strengthens communities, builds resilience and channels natural competitive instincts in a harmonious way.

Sport is a fundamental and true human value. This is the reason why the Office of Counter-Terrorism is proud to present this Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies. This Guide was developed as part of the UNOCT's Global Programme on the Security of Major Sporting Events, and the Promotion of Sport and its Values as a Tool to Prevent Violent Extremism, thanks with the invaluable partnership and support of the United Nations Alliance of Civilizations (UNAOC), the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the International Centre for Sport Security (ICSS). Its raison d'être is to help all relevant stakeholders, in particular policy-makers and practitioners, to prepare, organize and manage sporting events while mitigating the constantly evolving threats posed by terrorism.

This publication greatly benefited from the contributions of Member States, international organizations, regional organizations, sports associations, the private sector and academia, with special thanks to the the Counter-Terrorism Committee Executive Directorate (CTED); the International Criminal Police Organization (INTERPOL) ; the Fédération Internationale de Football Association (FIFA);  the Council of Europe (CoE); the Confédération Africaine de Football (CAF); the Asian Football Confederation (AFC); and the Union of European Football Associations (UEFA).

Finally, I want to express my gratitude to all the officials and partners who have supported the development of this document and offer my sincere appreciation for the contributions of the People's Republic of China through the United Nations Peace and Development Trust Fund, the State of Qatar and the Republic of Korea for their generous financial support, which has made possible this publication and the entire work carried out by the Global Programme.
Mr. Vladimir Voronkov
Under-Secretary-General
United Nations Office of Counter-Terrorism

**UNAOC**

The United Nations Alliance of Civilizations (UNAOC) is a proud partner of the Global Programme, together with the UN Office of Counter-Terrorism (UNOCT), the UN Interregional Crime and Justice Research Institute (UNICRI) and the International Centre for Sport Security (ICSS). UNAOC strongly believes in the power of sport to prevent violent extremism through its ability to break down walls between people regardless of their faith, race or culture. But people everywhere must be allowed to watch and practice sports in peace. This guide provides excellent guidance for key decision-makers when it comes to security at major sporting events at all stages of their organization, calling for active collaboration with relevant stakeholders, including community leaders and youth, due to their understanding of the local context.
H.E. Mr. Miguel Ángel Moratinos
High Representative for the United Nations Alliance of Civilizations

**UNICRI**

UNICRI is pleased to contribute to this Guide based upon our extensive expertise in the field of major events security, gained over two decades of technical assistance to more than 70 Member States. In 2006, UNICRI established the International Permanent Observatory on Security Measures during Major Events, welcomed by ECOSOC in its Resolution 2006/28. Through this framework, UNICRI has promoted the most effective methods to keep major events safe and secure around the world. We are proud to share our know-how and lessons learned with the Global Programme and to see the key elements we identified – namely, the importance of integrated planning, public private partnerships, community engagement, and regional cooperation – echoed in this important publication. This Guide perfectly illustrates how a holistic approach fosters the security of major sporting events for everyone to enjoy around the world".

Ms. Antonia Marie De Meo
Director of UNICRI

**ICSS**

This Guide crystalizes the experience of generations of policy and decision-makers, and their visions on how to plan the security of major sporting events, including with regard to legacy factors, sustainability and cooperation across sectors. It provides an exhaustive overview of all the forms of support and mutual assistance available within the international community to protect such events as a common good across nations, as a catalyst for change and a staging area for global citizens. ICSS feels proud to have shared the knowledge it has developed since its establishment and mobilized its community to arrive at a document which, we believe, represents a precious high-level orientation on the security challenges and opportunities to be considered from the very initial decision to bid to for a major sporting event.

Mr. Mohammed Hanzab
ICSS Chairman

## ACKNOWLEDGEMENTS

The United Nations Office of Counter-Terrorism (UNOCT), the United Nations Interregional Crime and Justice Research Institute (UNICRI), the United Nations Alliance of Civilizations (UNAOC) and the International Centre for Sport Security (ICSS) wish to sincerely thank a wide variety of experts and officials who contributed to this Guide on the Security of Major Sporting Events, Promoting Sustainable Security and Legacies.

The Guide represents a cornerstone of the security component of the Global Programme on Security of Major Sporting Events, and Promotion of Sport and its Values as a Tool to Prevent Violent Extremism, and its aim to protect major sporting events as a common good of the international community.

The Global Programme is made possible thanks to the generous contributions and support provided by the People’s Republic of China through the United Nations Peace and Development Fund (UNPDF); the State of Qatar and the Republic of Korea.

The Global Programme’s partners would like to express their sincere gratitude to Mr. Mauro Miedico, Deputy Director, Chief of UNOCT Special Projects and Innovation Branch, for his oversight and continuous impulse to the programme in all its components; and to Mr. Massimiliano Montanari, CEO at ICSS, for the strategic contribution given to the Guide and his supervision; and to Ms. Carol Jimenez, ICSS, for coordinating a drafting process which included an extraordinary community of committed experts and officials from the world of sport, security, academia and international cooperation.

A special thank goes to the chairs of the Task Groups which led to the completion of the Guide, including the Coordinator of the Global Programme, Mr. Valerio De Divitiis, UNOCT; Ms. Anne-Maria Seesmaa and Mr. Jean-Philippe Morange, CTED; and Mr. Duccio Mazarese, UNICRI; and to the the principal drafters and coordinators of the Task Groups, namely Mr. Esteban Giudici and Mr. Brendan Heffernan; ICSS officials Mr. Diogo Guia and Mr. Dale Sheehan, as well as Mr. Eddie Marshbaum, Mr. Stefano Betti and Mr. Brian London your expertise, knowledge and commitment have made this Guide a reality.

Mr. Richard Chalk, Mr. Travis Heneveld, Mr. Stuart Hodge, Mr. Howie Lodder and Mr. Giovanni Pisapia are kindly thanked for their expertise and contribution in the drafting of specific sections of the Guide.

A special thanks also goes to Mr. Alex P. Schmid and Ms. Anna Korula for their reviews and content integration.

Thanks go to the officials involved from the UNOCT Special Projects and Innovation Branch: Ms. Guadalupe Megre, Ms. Sereena Karsou and Mr. Khalil Otmane. Your support across the various moments of the drafting has been highly appreciated.

Further acknowledgement goes to ICSS staff members for all the research work conducted in support of the Guide: Ms. Magda de Lange for her precious analytical support, as well as to Mr. Fred Lord, Mr. Steven Fleming, Mr. Massimiliano Di Cola, Ms. Michelle Maxwell, Mr. Max Mumford and Mr. Alain Van Thiel, who are also greatly acknowledged for their much-appreciated contributions throughout this process.

In addition, the Global Programme would like to express its sincere gratitude to those experts and officials who actively participated throughout the process of the drafting of the Guide in both expert meetings and interviews and by responding to the consultation documents, namely Mr. Mahfoud Amara (College of Arts and Sciences at Qatar University); Mr. Antony Anderson (Jamaica Constabulary Force); Mr. Luis Manuel Andre Elias (National Police of Portugal); Mr. Maurizio Barbeschi (World Health Organization,WHO); Mr. Joseph Callixtus (Caribbean Community Implementation Agency for Crime and Security); Mr. Louis Chiasson, Mr. Augusto Coriglioni, Mr. Christian Emeruwa (Confederation of African Football, CAF); Mr. Paulo Valente Gomes (Council of Europe, CoE); Mr. Adam Lewis (Adidas); Mr Alphonse MacNeil; Mr. Francesco Norante (Leonardo Canada); Mr. Shahin Rahmani (Asian Football Confederation); Mr. Domenico Paterna, and Ms. Janet Williams (Supreme Committee for Delivery and Legacy).

Special thanks also go to those who participated in experts' interviews; your expertise and wealth of information have been most useful: Mr. Gregory Bujac (OSAC, U.S. Department of State); Mr. Richard Caborn (Minister for the London 2012 Bid and England FIFA World Cup 2018™ Bid); Ms. Jane Fernandes (Football Federation Australia); Mr. Alex Marshall

(International Cricket Council, ICC); Mr. Eloy Mazon (4Global); Mr. Alexander Protosov (2018 FIFA World Cup™ Russian Federation); Mr. Andrey Reis (FIFA™); Sir Mark Rowley (Former Senior Police and Assistant Commissioner for Specialist Operations of the Metropolitan Police); Mr. Peter Ryan; Mr. Andreas Schaer and Mr. Kenny Scott (UEFA); Ms. Katharina Steinberg (FIFA™); and Mr. Marc Timmer (UEFA).

A word of appreciation goes to those who participated as panellists in the Expert Group Meeting in New York on  3 and 4 February 2020, and to all providing valuable information and insight on the planning and implementation of an MSE: Mr. Ebrahem Abdulaziz Ali Al Mohannadi, (Ministry of Interior, State of Qatar); Mr. Fares M. Almalik (Brigadier, Kingdom of Saudi Arabia); Ms. Tonya Ayow (CARICOM Implementation Agency for Crime and Security); Ms. Eva-Maria Engdahl (European Commission Directorate-General, Migration and Home Affairs, Unit D2 – Counter-Terrorism); Mr. Carlos Fernandez (Central American and Caribbean Association Football); Ms. Paola Fernandez (Organization of American States); Ms.  Sandy Harvey (Federal Policing National Security of Canada); Mr. Eric Heip (Ministry of Interior of France); Mr. Jay Jadeya (Football for Peace); Mr. Changmin Kim (Ministry of Interior and Safety, Republic of Korea); Mr. Hyun-tae Kim, (National Counter-Terrorism Center, Republic of Korea); Mr. Kevin LeClair (VISA); Mr Aldric Ludescher (International Olympic Committee, IOC); Mr. Jorge Gonçalves Mauricio (INTERPOL); Mr. Donal McCarthy (Uber); Mr. William G. Raisch (International Center for Enterprise Preparedness, New York University); Mr. Tofig Seyfullayev (Deputy, INTERPOL Division, National Central Bureau, Ministry of Interior, Republic of Azerbaijan); Mr. Helmut Spahn (FIFA™); Lord John Stevens (ICSS Board Member); Ms. Hilde Vandevoorde (Eurojust); and Mr. Philip Walker, (OSAC, U.S. Department of State).

The Global Programme would like to acknowledge the assistance of all governmental authorities, business sector, academic and international experts who participated in the Task Groups. These Task Groups contributed to gathering critical and relevant information through different consultation documents: Mr. Hans Das (European Union); Ms. Daniela Giuffre (Provincial Street Police, Pistoia, Italy); Mr. Jesus Gomes Hernandez (National Police of Spain); Mr. Arturo Gonzalez (United Nations Office on Drugs and Crime, UNODC); Mr. Brian Johnson (Asian Football Confederation); Mr. Edgar Moreno (Vice President Global Security, Telemundo Enterprises & Latin America); Mr. Denys Movchan (Ministry of

Internal Affairs in Ukraine); Mr. Guenther Sablattnig (European Union); and Ms. Andrea Volkmer (European Commission).

We also acknowledge the support provided by Mr. Keitaro Aoki (Asian Football Confederation); Mr. Rod Buckingham (Canadian Football League); Mr. Ronnie Francis M. Cariaga (Philippine National Police); Mr. Miguel Angel Diaz Monzon (Spanish Guardia Civil Police Force); Mr. Denis Movchan; and Ms. Kamilla Swart-Arries (Hamad Bin Khalifa University).

In addition, the Global Programme would like to thankfully acknowledge the contribution of the panellists who contributed exclusively during the virtual meeting on "The Impact of COVID-19 on the Security of Major Sporting Events"; your contribution helped to identify good practices and to foster a global conversation on the impact of health regulations on Major Sporting Events: Mr. Falah Al-Dosari (INTERPOL); Mr. Erik Bekaert (Ministry of Interior, France); Mr. Maxime Bornon (Ministry of Interior, France); and Mr. Mike Hopmeier (Unconventional Concepts, Inc).

Finally, the Global Programme thanks Mr. David Winch for having edited this Guide in a manner that enhances its accessibility for readers from different sectors and backgrounds.

## KEY RECOMMENDATIONS

Following the structure of the Guide, this section consolidates the recommendations featured at the end of each chapter. It provides an overview of key steps and approaches for decision-makers to consider in the security domain during the preparations and execution for an MSE.

### FOUNDATIONS OF SECURITY AT MAJOR SPORTING EVENTS (Chapter III)

#### Leadership and Vision

→ Select leaders in charge of the security of MSEs based on a proven track record of ethical and moral behaviour.

→ Ensure that leaders in the security field act strictly within the law and that they are fully committed to the values of diversity, inclusiveness, gender and racial equality.

→ Include the security mission within the broader vision for the MSE and align security considerations to the MSE's core organisational values.

#### Coordination

→ Plan and manage the security process for an MSE by involving a wide range of national authorities (e.g. Ministries of Interior, Justice, Defence, Security, Foreign Affairs, Sport, Treasury, Planning, Transportation and Health) in the decision-making process.

→ Ensure that security coordination efforts reflect multi-level institutional arrangements in the hosting country (roles and responsibilities of national and local levels of Government in the security arena).

→ Include the business sector and civil society in security-related decision-making processes.

→ Ensure that security planning and management are supported by adequate legal and regulatory frameworks outlining, inter alia, clear and smooth procedures aimed at the identification of roles, timelines as well as hierarchical and reporting mechanisms.

→ Engage highly qualified staff to work on safety and security tasks and provide them with specialized training on the implications of handling an MSE. Staff from private security agencies, when recruited, should also undergo appropriate training.

→ Make inter-agency coordination efforts effective by establishing interoperable databases, communication and information-exchange systems.

**Continuity**

→ Plan for security (e.g. budgets, human resources) in a sustainable and realistic manner by minimizing risks that the time gap between the planning and the delivery time that affect the quality and extent of security eventually delivered.

→ Ensure that the security objectives are fully understood, endorsed and acted upon by all stakeholders throughout event planning and delivery, particularly in cases of personnel changes.

→ Establish mechanisms to continually evaluate the proper functioning of security systems and processes as well as their continued relevance in the face of a changing security environment, technological advances, institutional restructuring, etc.

**Cooperation**

→ Promote an environment whereby all stakeholders with security-related responsibilities share the same values and collaborative spirit, in line with the notion of joint participation in a multiagency and multisectoral approach.

→ Encourage the voluntary and pro-active sharing of knowledge and technical support between all stakeholders involved in security planning, organizing and delivery.

**Communication**

→ Develop and actively promote a comprehensive communication strategy accessible to all stakeholders performing security-related tasks in relation to the MSE, both from the public and the private sector.

→ Set up the adequate infrastructure and information/communication technologies for the timely and secure exchange of operational information within participating agencies.

→ Implement a process of continuous consultation throughout the MSE event cycle to regularly integrate security-related feedback from all stakeholders.

**Good Governance**

→ Ensure that principles underpinning “good governance” inform all phases of the security-related decision-making processes for an MSE.

→ Establish solid good-governance models and ensure their dissemination across the whole spectrum of agencies involved in security-related tasks for an MSE.

### Proper Estimate of Security Costs

→ Carry out an initial estimate of security costs as early as possible during the event-planning process in light of an assessment of the capacity of a country/city to host the event and protect it from foreseeable threats and disruptions.

→ Account for costs involved in the protection not only of venues hosting the competition but also enabling critical infrastructure (e.g. electricity distribution networks) and potential soft targets surrounding the competition area (e.g. crowded bars where fans may gather).

→ Provide for sufficient budget contingencies to address change variances to the original planning assumptions.

→ If resort to private security firms is envisaged, budget costs for recruitment, training uniforms, equipment, accommodation and transport purposes.

→ Frame security costs as medium- and long-term investments for the benefit of the community as opposed to expenses solely needed to secure a one-time event.

## SECURITY CONSIDERATIONS BEFORE AND DURING THE BIDDING PROCESS (Chapter IV)

→ Conduct security-related assessments (challenges, threats, opportunities, cost implications) right from the exploratory stage, and foresee the holding of successive assessments over time as the event draws nearer, also in order to factor in new and emerging threats.

→ Where appropriate and feasible, leverage predictive analytics and artificial-intelligence-based models as tools to sharpen the quality and precision of security-related assessments.

→ Choose venue locations as soon as possible, utilizing input and trend analyses by law enforcement agencies at an early stage. Site selection should be influenced by factors such as, inter alia, crime hot spots and neighbouring high-risk communities.

→ Set up a Technical Bidding Team and develop effective working relations with international security and law enforcement agencies such as the International Criminal Police Organization (INTERPOL) and regional bodies.

→ Carry out a thorough analysis of the technical security requirements outlined in the bidding document in order to determine levels of needed resources and anticipate levels of socio-economic disruption and impact to local communities in the lead-up to, and during, the MSE.

→ Carry out an advance estimate of the type and level of military/law enforcement resources that will be effectively available for deployment to the MSE (e.g. consider contingents that may have already been earmarked for International Peacekeeping Missions, impacting the number of resources deployable to the MSE).

**LEGAL AND INSTITUTIONAL FRAMEWORKS (Chapter V)**

→ Undertake an early-stage, comprehensive review of the legal preparedness of the country to host the MSE, considering, in particular, the time needed for legislative/regulatory overhauls to be enacted through the country's normative and bureaucratic processes.

→ In conducting the above-mentioned legal review, in particular, determine gaps and needs for reform in terms of a) whether the domestic legal framework is sufficiently equipped to prevent and counter-terrorism and other criminal conduct potentially affecting the organisation of an MSE; b) whether adequate regulations are in place governing security planning and management of an MSE; c) whether national legislative and institutional frameworks provide for effective measures and safeguards to comply with international human rights standards (e.g. legality, proportionality, non-discrimination).

→ Determine the extent to which legal enhancements should be introduced via legislation/ regulation explicitly focusing on the forthcoming MSE as opposed to the adoption/amendment of generally applicable normative tools (e.g. criminal codes).

→ As part of the preparations for an MSE, consider priority ratification (where applicable) and/or implementation, of the following instruments:

- Universal (UN) legal instruments for the prevention and suppression of international terrorism;
- UN Convention against Transnational Organized Crime, and its Protocols;

- Council of Europe Convention on Cybercrime;
- United Nations Global Counter-Terrorism Strategy;
- Security Council resolution 2341 (2017) on protection of critical infrastructure against terrorist acts;
- Security Council resolution 2396 (2017) on foreign terrorist fighters, and the 2018 Addendum to the 2015 Madrid Guiding Principles (Foreign Terrorist Fighters);
- Council of Europe Recommendation Rec (2015) on Safety, Security and Service at Football Matches and other Sports Events;
- Council of Europe Convention on an Integrated Safety, Security and Service Approach at Football Matches and Other Sports Events;
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism;
- Council of Europe Convention on the Prevention of Terrorism;
- European Convention on the Suppression of Terrorism;
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime;
- European Convention on the Compensation of Victims of Violent Crimes;
- Council of Europe Anti-Doping Convention; and
- Council of Europe Convention on the Manipulation of Sports Competitions

## STAKEHOLDER COOPERATION (Chapter VI)

### General principles

→ Understand "stakeholder collaboration", based on shared values, as a prerequisite for MSEs to result in a secure environment. Ensure that close and effective levels of stakeholder collaboration are established in the very early planning stages and are maintained right into the post-event phase.

→ Engage and encourage a wide range of stakeholders to share their particular security-related concerns (e.g. national police, fire department, Red Cross, health authorities, participating sports organizations, and authorities responsible for sports venues, logistics, civilian protection, volunteers, VIPs private and public security, transportation (air and road), cyber and information technology).

- → Conduct a capacity assessment, with input and analysis provided by multi-disciplinary subject matter experts, to determine the capabilities of each partner and to provide a roadmap for building the required overall security capacity.
- → Provide vetting systems for individuals directly involved in security planning and implementation.
- → Establish security protocols for construction, venue setup, catering, cleaning, volunteers, and transport areas. Such protocols may address communication strategies, training, staff-vetting requirements and site-access authorizations.

**International cooperation and outreach**

- → Ensure that threat assessments by national intelligence and security services are conducted in close and regular consultation with international partners, including countries from where a significant influx of fan groups is expected.
- → Consider the signing of specific bilateral and/or multilateral agreements with international partners as a tool to cement cooperation and support concrete actions in the run-up to and during the MSE.
- → Leverage the often-extensive assistance that international and regional organizations can offer to countries in planning and executing security measures before and during an MSE.
- → Involve all countries represented at the MSE in security preparations and in resource-sharing as a condition to enhance security capacities and reduce potential threats and risks.

**Information sharing**

- → Support stakeholder collaboration by establishing effective information-sharing arrangements, including by a) setting up an information-technology platform that is compliant with applicable regulations and that can be used to share data securely and seamlessly between stakeholders; and b) setting up event-specific platforms for participating countries where relevant security information can be collected and analysed.
- → Use the secure channels offered by international and regional law enforcement organizations to exchange operational information with other countries.

**Engagement with the private sector**

- → Develop functional public-private partnerships (PPPs) to enhance security and to safeguard the public during MSEs.
- → Encourage stakeholders from the private sector to contribute to inclusive information exchange with a view to sharing risk assessments, adding value/efficiency/depth to the security dialogue as well as, where appropriate, developing security solutions. Public-private information sharing should be supported by the conclusion of specific agreements.
- → Throughout the security planning and implementation process, involved in the discussion owners and managers of a) critical infrastructure that will deliver essential services to the MSE, b) sites (e.g. soft targets) which may become targets of attacks in relation to the MSE.
- → Hold regular security briefings between sponsors, security organizers and law enforcement authorities with a view to, among others: a) discussing potential security measures to protect sponsors who may become targets of criminal or terrorist attacks; b) exploring how sponsors can contribute to security planning and operations; c) leveraging sponsors' marketing expertise to develop appropriate messaging around security measures.

**Engagement with civil society**

- → Recognize the crucial role that civil society (in the form of local communities, non-governmental organizations, supporter organizations, and influential individual spectators) plays in the security planning of MSEs and determine in advance what civil society can contribute when dealing with the aftermath of security-related incidents.
- → Encourage stakeholders from civil society organizations to contribute to inclusive information exchange with a view to sharing risk assessments, adding value/efficiency/depth to the security dialogue as well as, where appropriate, developing security solutions.
- → Work with NGOs, including local social-justice organizations, to a) share knowledge, build capacity and increase accountability around critical human rights issues; b) obtain advice on how issues such as racism, discrimination, poverty, or civil rights can be considered as part of security preparations and operations.

→ Develop interaction with supporters' organizations to inform best practices as a way to minimize conflict between fan groups or backlash against security personnel.

## THE SECURITY PLANNING (Chapter VII)

### General principles and governance

→ Understand security planning as a prerequisite to ensure that operations become executable, sports competitions take place without disruptions, and the experience is positive for all present. At the same time, ensure that security complement, as opposed to hinder, the overall event experience.

→ Ensure that authorities in charge of security define their vision for the security operation in line with the overall mission and strategy for the MSE. All contributors should understand and adhere to that vision.

→ Plan for security as a "whole of government" effort, beginning as early as possible and broadly involving all stakeholders with roles and responsibilities in the security domain, including the MSEs' local organizing committee and the business sector.

→ Ensure that one Ministry act as the Government's lead security agency responsible for the MSE.

→ Ensure that the security planning system brings together multiple agencies with diverse backgrounds and engage them at various levels as executive leaders, senior leaders, mid-level managers and tactical planners.

### Leadership

→ Ensure that security leaders are prepared to embrace and build trusted relationships and to take a conciliatory approach when dealing with competing or conflicting issues.

→ Recruit a lead security planner with strong experience in strategic planning, risk and project management.

### Strategic approaches to security planning

→ Ensure that the level of visibility of the security apparatus - although discreet – remain noticeable by attendees, acting both as a deterrent against possible malicious acts and conveying a sense of protection.

- → Develop adaptable and scalable security plans (up/down in terms of scope and resources) to respond to a fluid and evolving threat landscape in the course of the planning phase.
- → Plan for worst-case scenarios (e.g. terrorist attacks, violent protests, natural disasters such as earthquakes) in the framework of an "all hazards" approach, while also preparing for more probable crime situations and incidents.
- → Throughout the planning cycle, subject security plans to testing and validation with robust exercises in order to declare a state of operational preparedness.
- → Categorize plans into groups, which allows for a systematic management approach to ensure interoperability and ensure more effective use of resources as plans evolve.
- → Consider a layered approach for the protection of MSE's venues and other sites.
- → Run a 'Knowledge Transfer Process' from the very start of the planning phase as a way to capture key insights gained from the entire MSE project, so that future planners can reduce risk and costs based on lessons learned.

**Security Design**

- → Design security from the start, and base it on international standards and best practices, in order to prevent costly redesign or ineffective security solutions.
- → Approach the security design as a multi-disciplinary endeavour, with security designers liaising with architects, landscape architects, mechanical-electrical-plumbing (MEP) engineers, ICT engineers, fire and life safety (FLS), crowd modelling, transport modellers, lighting engineers etc.
- → Designs should be agreed upon at each stage before the security design is undertaken to minimize any potential risk to redesign.

**Planning for resource management**

- → Use existing infrastructure and equipment to the greatest possible extent to reduce costs and procurement delays.
- → Facilitate opportunities for joint procurement, i.e. when multiple LOC or government entities may require the same good or service (e.g. acquisition of hotel rooms or hospitality requirements)
- → Ensure that the integrated multi-organizational security system has a built-in mechanism to ensure that plans are interoperable.

- → Consider involving law enforcement entities such as the coast guard, park rangers, conservation officers, fisheries' officers or any other capable professional national/regional/local law enforcement officials to enhance security and create a force-multiplying effect.
- → Consider utilizing professional and well-trained private security personnel as officials

**COMMUNICATION STRATEGIES (Chapter VIII)**

- → Design a strong internal and external communication strategy aimed at a) building and maintaining public confidence in the security measures; b) engaging in transparent and timely interactions with the media and other external stakeholders; and c) providing timely communications, both internally and externally.
- → Set up an Integrated Security Communication Team (ISCT) with the responsibility of sharing information and addressing communication/media issues that may affect the security of the MSE.
- → Channel all requests for external communications through the ISCT to ensure consistency and avoid conflicting messages.
- → Develop a strategy to communicate with the public audience during all stages of the MSE life cycle as well as the planning phase.
- → Set up a Community Relations Group (CRG) in charge of establishing and maintaining open and transparent lines of communication with all stakeholders who may be affected, directly or indirectly, by the preparations for the MSE (e.g. local business operators and community residents).
- → Create a Community Activist Liaison (CAL) to ensure that there is an ongoing dialogue with activists and that their right to protest is acknowledged while being informed of police expectations, actions and consequences. CALs can be used to help enforce designated, agreed-upon protest areas.
- → Keep the media abreast of facts and situations impacting the broader public interest.
- → Plan to directly engage local media and the public to address concerns as to how the event might affect the local community.

**SECURITY IMPLICATIONS OF CO-HOSTING MAJOR SPORTING EVENTS (Chapter IX)**

- → Set up joint preparations well in advance, including the establishment of agreements between Governments and relevant multinational working groups
- → Develop a clear overall police strategy and coordination structure
- → Create Memorandums of Understanding with participating, transit, and neighbouring countries and with other international organizations
- → Harmonize security-related legislation between host nations
- → Design a harmonized border control framework
- → Harmonize media and communication policies related to security arrangements
- → Organize study visits to share practical experiences
- → Harmonize Public-Private Partnerships with cross-border application

**THE IMPACT OF COVID-19 ON THE SAFETY AND SECURITY OF MSEs (Chapter X)**

- → Include crises and disaster contingency-planning in the Host Authorities' preparations
- → Consider guidance documents by the main international health and sport governing bodies
- → Take great precautions and make special arrangements as long as mass vaccination against COVID-19 is not universally administered.

**LEGACY CONSIDERATIONS (Chapter XI)**

- → Ensure that the strategies, infrastructure, policies and institutional arrangements specifically put in place for an MSE continue to have significant and produce positive systemic social and economic impacts beyond the event itself.
- → During the planning stage, in particular, consider how the full range of security-related measures and arrangements can be designed and implemented in order to:
    - Consolidate legal and institutional frameworks in light of international standards;
    - Further develop a city or country's infrastructure, including modernizing facilities, venues, transport systems and related security components;
    - Consolidate the relationship between governmental agencies and the private sector based on the initial partnership experience created by the MSE;

- Integrate a human-rights-based approach into the design, implementation, monitoring, and evaluation of security policies;
- Improve the economic and social outlook of members of disadvantaged communities following, in particular, the employment opportunities generated by the MSE; and
- Facilitate urban development or regeneration.

# INTRODUCTION

Major Sporting Events (MSEs) are not just athletic competitions but also collective celebrations of human achievements and a source of pride for those who participate in them or host them. In recent years, the range of countries which have been prepared to organize an MSE has extended across all continents. Satellite-supported live television has broadened the number of spectators to hundreds of millions of people who watch and enjoy not just the MSE itself but also related events. This allows an organizing country or city to place itself, as it were, on the mental map of global audiences. This, in turn, can bring increased tourism, new or improved infrastructure, foreign investments as well as other benefits to those countries which manage to successfully showcase a major sporting event.

However, there is a downside to the opportunity to present itself to the world by organizing an MSE. If the organization is below the standards expected by athletes and the public, this might project a negative image of the country to the world. There are also external factors which can harm the image of an MSE and the way it will be remembered – its legacy. This could be prompted by a breakdown in security caused by an external threat: a terrorist assault or a criminal cyberattack, to name but two major risks.

With this in mind, the Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies contains an exhaustive analysis of all elements for consideration by key decision-makers when it comes to security at MSEs. Consistent with the relatively recent democratization of the access to organize and host MSEs outside traditional regions, this Guide is published in a context where the net is cast wider for those cities and countries looking to host MSEs. Intercultural and cross-regional complexities and particularities are dissected, providing a systemic overview of the main considerations for key decision-makers for the security elements of MSEs.

After setting out the broad context, the Guide offers an in-depth analysis of the political, social and financial dimensions of MSEs. After all, no country is immune to present-day security threats, and there are many threats to the security of society that cannot, and should not, be addressed in isolation. But when it comes to MSE security, “one size does not fit all.”[1] Every event will face a unique threat environment and differing capacities and approaches to manage

[1] Horizon 2020 PASAG, 2017, EU, 2018

those threats, and these will be influenced by the political, social and economic conditions in which the MSE is taking place. There are also differences in the security uncertainties for different types of events, which we will explore in more detail in these sections below.

Having ascertained the particularities of MSE hosts and their situation and geopolitical climate, it is important to examine the hallmarks of an efficient MSE security operation. The presentation of the security plan will be a showcase of leadership and vision from the MSE host representatives and should demonstrate the prioritization of *coordination, continuity, cooperation and communication* (the 4 Cs). It should be built on a solid foundation of good governance and transparency and will be predicated on a realistic, accurate and proportionate estimate of the costs of an effective security operation for the MSE.

All of these foundational measures will take place at the very preliminary phases of the MSE cycle. In fact, due consideration to security must be given right from the outset, well before a Bid has even been put together. During this exploratory phase and then into the bidding process itself, a potential host should have a solid foundation and idea of what the security proposal will look like in the relevant bidding documents.

Once hosting rights have been awarded and until the delivery of the event, solid legal and institutional frameworks must be in place in order to ensure that the MSE run in a secure manner. These frameworks may well move into the international sphere and will require a careful interface between the relevant sport's governing body, local authorities and national legislators in the Host Authority.[2] Careful consideration must be given to the legal implications of hosting an MSE, ranging from issues such as counter-terrorism, crowd control, intelligence interface and MSE security operations. These must always be counterbalanced against fundamental respect for human rights. Furthermore, the MSE can be an opportunity for a city or country to upgrade its legislation in order to have a lasting effect, well beyond the event cycle itself.

A full chapter is devoted to stakeholder cooperation, dissecting the intricacies of inter-agency, international and multisectoral cooperation. Each of these areas of cooperation has nuanced application to the security of MSEs and will each be paramount to deliver a secure MSE. As at the planning and operational levels, this cooperation should be well thought out and executed.

[2] Host Authority: The entity or authority responsible for organizing an MSE. May refer to the city, region or Government of country or an organizing body. In most cases, the Host Government will refer to a public entity whereas the Host Organizing Committee will be private.

Indeed, the MSE will be an opportunity to establish solid foundations for these forms and levels of cooperation, and to create a legacy for the host city and country for the benefit of all. Furthermore, part of the cooperation process is the intrinsic concept that knowledge should be transferred from one MSE to the next. As explored in more detail in Chapters VII and VIII, organizing an MSE is a collective endeavour that must engage all relevant partners and agencies. Technical expertise must be guarded and passed on between organizing committees – foundations of effective multi-stakeholder cooperation.

With this sophisticated stakeholder cooperation in place and functioning smoothly, the system and deliverables of security planning for the actual MSE are put in place. Planning and organizing an MSE represents an exceptional challenge for any host country or city due to the number, complexity and multidimensional nature of the matters that this type of events involves. The organizing authorities are also frequently affected by tight timelines and specific expectations of different stakeholders and participants, such as spectators, athletes, dignitaries and journalists.[3] Along with these intricacies, MSEs may attract unnerving threats, such as terrorism, hooliganism, organized crime and cybercrime, which need to be duly attended. In this context, it is clear that planning and delivering the security of an MSE requires the coordination of several activities and actors.

Chapter IX looks at some security recommendations when co-hosting major sporting events – i.e., the relatively modern phenomenon of multiple countries hosting MSEs, including the UEFA EURO jointly hosted by Poland and Ukraine in 2012 or the Australia and New Zealand FIFA Women's World Cup 2023. Such events will have their own challenges when it comes to delivering an effective security operation – largely to do with cross-border and cross-cultural considerations, expectations of sporting federations, cooperation between authorities across borders, and security implications of associated logistical challenges of multi-national events.

Chapter X reorients the Guide, delving into the impact of COVID-19 on the world of sport and MSEs, and what this means for security for events in the future, before dealing with the general areas of communications strategies and post-event evaluations.

Finally, the concept of legacy is addressed, focussing primarily on the *security* legacy of MSEs. For this element, we borrow the words of the founder of the modern Olympic Games:

[3] Giovanni Pisapia (2006). Major Sport Events Safety and Security Framework´s Core Elements. *International Journal, Italian Team for Security, Terroristic Issues & Managing Emergencies, issue 2/2016, p. 139/158.*

> *"It would be very unfortunate, if the often exaggerated expenses incurred for the most recent Olympiads, a sizeable part of which represented the construction of permanent buildings, which were moreover unnecessary – temporary structures would fully suffice, and the only consequence is to then encourage the use of these permanent buildings by increasing the number of occasions to draw in the crowds – it would be very unfortunate if these expenses were to deter (small) countries from putting themselves forward to host the Olympic Games in the future."*[4]
>
> (Pierre de Coubertin, 1911)

While the Guide is primarily focused on the security element of legacy, these words ring true in the modern era, over 100 years after they were uttered. When making these investments in security in the context of an MSE, one must always have the bigger picture in mind, thinking about future positive effects for Host communities.

[4] See https://stillmed.olympic.org/Documents/Reports/EN/en_report_725.pdf, p.3.

# I. THE GUIDE

## 1. Aim, Scope and Target Audience

The aim of the Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies is to provide a comprehensive overview of the challenges and opportunities that organizing an MSE implies for the host authority and the international community, specifically from a security perspective.

Security, in the context of an MSE, refers to the design of mechanisms and measures which can offer protection against potential harm to athletes, spectators, support staff, and dignitaries. Security planning focuses on the prevention of malicious acts and the preparation of rapid intervention mechanisms and mitigation measures to manage incidents which can stand in the way of conducting a safe and peaceful event.

The Guide considers the inter-links between security[5] and various safety measures[6] and services[7], as defined by the Council of Europe's Saint-Denis Convention, aspects of which could have an impact on the final outcome of the event from a security perspective.

This Guide reviews MSEs ranging from the Olympic Games and FIFA World Cup™ tournaments to any other international, continental/regional or multinational sports competitions which require international security cooperation and involve mass gatherings.[8] It

[5] The concept of **security** incorporates all measures designed to deter, prevent and sanction any incident of violence or misbehaviour in connection with football or other sport events – inside or outside of a stadium. The concept of ***security*** includes, in particular, risk assessment, co-operation between police and other relevant agencies and the establishment of sanctions.See https://www.coe.int/en/web/sport/a-multi-agency-integrated-approach

[6] The concept of **safety** combines measures related to the protection of people from being injured or facing a risk to their health and well-being during sports events. This comprises stadium infrastructure and certification, contingency plans or measures regarding the consumption of alcohol. Safety measures also protect people on their journey to the event and in public viewing areas outside stadiums.See https://www.coe.int/en/web/sport/a-multi-agency-integrated-approach

[7] The concept of **service** comprises all measures designed to make sport events enjoyable and welcoming for all, in stadiums but also in public spaces where spectators and supporters gather before, during and after the event. This includes material aspects such as good catering and toilet facilities; but, above all, it focuses on the manner in which people are welcomed and treated throughout the event. See https://www.coe.int/en/web/sport/a-multi-agency-integrated-approach

[8] UNICRI's IPO Planning Model provides a definition of **major events**, listing a number of characteristics that well describe major sporting events: historical, political significance or popularity; large media coverage and/or international media attendance; participation of citizens from different countries and/or possible target groups; participation of VIPs and/or dignitaries; large number of persons attending and the potential posed by threats, therefore requiring international cooperation and assistance.See http://www.unicri.it/topics/major_events_security/the_house

strongly promotes approaches for ensuring that the security-related arrangements put in place for a specific MSE leave a long-lasting legacy in the security capacity of the Host Authority, while also contributing to the promotion of human rights and socio-economic development.

In this sense, the Guide offers a holistic view of the main security aspects that should be taken into account by policy and decision-makers when considering the feasibility of hosting an MSE in their country with the aim of promoting the adoption of advanced policies and the creation of eco-systems to better identify, understand, prevent and counter threats, thereby also mitigating risk of incidents of violence in the context of MSEs.

The Guide seeks to provide information on national experiences as well as on existing international cooperation mechanisms; it does this by collating and analysing available guidelines and instruments on the topic. It also serves as a reference document to increase the level of preparedness to adequately address potential attacks or adverse situations that might affect an MSE, including sites, infrastructure and people.

The advice contained in this Guide is intended to provide an overview of best practices, experiences and opportunities available at the international, regional and national levels to provide security at MSEs. It recognizes the different context in which various MSEs take place, and therefore is mindful of divergent cultures, legislative frameworks and levels of available resources, all of which will inevitably affect the way the security operation of an MSE is conducted. While the Guide does not seek to provide prescriptive or definitive models, it should be seen as an integral and specialised  part of the guidance and reference tools being developed in the framework of  UNOCT’s Global Programme on the Protection of Vulnerable Targets against terrorist acts.[9]

The Guide serves primarily as a reference document for a wide range of stakeholders, particularly policy- and decision-makers from national and local governmental agencies, having responsibilities for the planning, organization and implementation of MSEs, or playing a role in the exploratory phase; they are hereafter referred to as the Host Authority. The Guide

WHO defines a mass gathering as  “a planned or spontaneous event where the number of people attending could strain the planning or response resources of the community or country hosting the event”. See https://www.who.int/news-room/q-a-detail/what-is-who-s-role-in-mass-gatherings

[9] Under the Global Programme, in particular, UNOCT is partnering with CTED, UNAOC and UNICRI (in close consultation with other organizations, including INTERPOL) to elaborate four good practices manuals on the protection of urban centres, tourist venues, places of worship as well as the threat posed by unmanned aerial systems. UNOCT is also in the process of drafting a modular Addendum to the Compendium of Good Practices on the protection of Critical Infrastructure, developed by UNOCT and CTED in 2018.

may also be used by non-governmental and business entities that are involved in various ways in supporting the planning effort of an MSE from a security perspective, including decision-makers from international, regional and national sports federations, bidding committees, organizing committees and any other relevant stakeholders.

The recommendations, key steps and approaches contained in this Guide may be used equally by national Government authorities or international sports federations (ISFs), as well as by local government authorities or regional sports entities, from the on-site operational level to the national Government level.

## 2. Threats

The Guide identifies a number of criminal threats, including terrorism, which can disrupt the successful conduct of MSEs, including emerging ones such as the use of unmaned aircraft and cyberattacks against facilitites or structures integrated to the MSE. Due to the global exposure generated by and associated with MSEs, including the presence of media from all over the world, attacks against MSEs – both physical and virtual - are attractive to a number of malicious actors. These can range from individuals using ICT systems to hack the internal communication channels of MSEs from their homes to sophisticated criminal and terrorist organizations which plan kinetic attacks using a wide spectrum of weapons and tools, including chemical, biological radiological and nuclear (CBRN) material.

For the purposes of this Guide, the main security threats to MSEs include, but are not limited to:

- Conduct defined by the Universal Instruments related to the Prevention and Suppression of International Terrorism;
- Breaches against public order and other offending behaviour (based on the legal framework of the hosting country);
- Conduct defined by the United Nations Convention against Transnational Organized Crime (UNTOC, or Palermo Convention) and its Additional Protocols; [10]

[10] United Nations Convention against Transnational Organized Crime and the Protocols Thereto; see https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .

- Cyberattacks, i.e. crimes committed via the Internet and other computer networks as defined by the Council of Europe Convention on Cybercrime;[11]
- Maliciously-induced health hazards such as the release of toxic substances in public places;
- Emerging threats, e.g. drone attacks on stadiums or infrastructure relating to MSEs, during or in the lead up to sporting events; and
- Conduct defined by the Council of Europe Convention on the Prevention of Terrorism.

### Why Would Terrorists Target a Major Sporting Event?

In 1975, the American terrorism expert Brian M. Jenkins said: "Terrorists want a lot of people watching and a lot of people listening and not a lot of people dead".[12] Three years earlier, up to 800 million people had been watching the Munich Olympic Games on television worldwide. For the eight Black September terrorists attacking and killing 11 Israeli athletes, this large audience was probably the main reason they selected the site of the 1972 Olympic Games as their target location.[13]

This raises the question of how terrorists, in general, decide on target selection. To understand this, it is useful to distinguish between four different types of terrorist targets:[14]

1. Physical targets of violence (the direct victims),
2. Psychological targets of terror (persons identifying with actual victims),
3. Targets of (coercive) demands (usually governments), and
4. Targets of attention (one or more audiences).

Focusing only on the direct victims of terrorist violence misses the deeper meaning of terrorist attacks. Yet without actual physical victims, the terrorists' violent message would not get a broad hearing and would therefore miss what often is the main objective. The number of potential terrorist targets is almost endless, and if one soft physical target is hardened, terrorists can pick the next one from a seemingly unlimited number of soft targets. In other words, displacement can make the hardening of specific targets a futile task as terrorists can move from a highly protected site to a low-security location (e.g. from a sports stadium to the queue in front of the ticket office outside). For many, probably most terrorists, the important goal is to show their presence to the world on-air and online. In other words, what matters to them is whether their attack ends up being widely reported and covered on television, and nowadays also on social media via the Internet. In our interconnected world, the physical location where a news-generating event takes place has often become

[11] Budapest (2001) Convention on Cybercrime: see https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 .

[12] Brian Michael Jenkins, "International Terrorism: A New Mode of Conflict," in David Carlton and Carlo Schaerf (eds.), *International Terrorism and World Security* (London: Croom Helm, 1975), p. 15.

[13] Alex P. Schmid and Janny de Graaf. *Violence as Communication. Insurgent Terrorism and the Western News Media*. London, Sage, 1982, p. 30.

[14] Alex P. Schmid. *Political Terrorism*. Amsterdam: North-Holland Publication, 1984, p. 111.

secondary. Having said that, terrorists like to strike wherever many journalists and reporters are present, and major sporting events that are broadcast live worldwide are therefore at risk of becoming targets of terrorist attacks.

*Source*: Alex P. Schmid. *Layers of Preventive Measures for Soft Target Protection against Terrorist Attacks*. Chapter 27 in: Alex P. Schmid (Ed.). Handbook of Terrorism Prevention and Preparedness. The Hague: ICCT, 2020/2-21 (forthcoming).

## Terrorist Threat from the Sky? Drones Looming on the Horizon

While terrorists have been hijacking passenger planes since the 1960s and have also crashed a few of these into crowded places – most notoriously in the case of the attacks of 11 September 2001 in New York and Washington, D.C. – since 2016 a new threat has arisen: the terrorist use of weaponised unmanned aerial vehicles (UAVs), better known as 'drones'. So far, drone attacks have not caused mass casualties, but some of them were directed at civilian rather than military targets. More than 70 per cent of these attacks successfully reached their intended targets. This indicates that defence against armed drones flying under the radar is a problem for which counter-measures are only beginning to be developed.

When it comes to MSEs, one source of concern is drone-based explosive attacks on dignitaries and VIPs, e.g. during the opening ceremony of an MSE.

A risk-based scenario for the organizers of an MSE is an attack on a stadium full of athletes and spectators, with one or several drones releasing biological agents while flying over spectators and athletes. In 2019 France's Anti-Terrorism Unit UCLAT warned in a confidential report of "a possible terrorist attack on a football stadium by means of an unmanned drone that could be equipped with biological warfare agents" – an emerging threat reiterated by Julian King, the European Union's Security Commissioner.

The contamination of people and the venue itself might not only disrupt the MSE but also cause reputational damage to the Host Authority. While several drone-fighting systems have already been developed, using technologies like radio frequency-jamming and laser beams, their use in or near crowded places is untested and possibly problematical. If not one, but a whole swarm of drones (some armed, some not) were to attack a sports stadium simultaneously, even a sophisticated defence system might be overwhelmed. The risks of drone attacks with chemical, biological, radiological and nuclear (CBRN) materials might still be low, but the negative consequences can be high. While it makes sense to prepare security for MSEs mainly with an eye on high risk/low consequence attacks, low risk/high consequence attacks with CBRN materials cannot be ruled out.

Sources: Haugstvedt, Håvard, and Jan Otto Jacobsen. "Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors' Use of Weaponised Unmanned Aerial Vehicles (UAVs – 'Drones')", *Perspectives on Terrorism*, Vol. XIV, Issue 5, October 2020 (forthcoming)

Doffman, Zak. “Warning Over Terrorist Attacks Using Drones Given By EU Security Chief - Liteye Systems, Inc.” Liteye Systems, Inc, 4 Aug. 2019: see https://liteye.com/warning-over-terrorist-attacks-using-drones-given-by-eu-security-chief/.

## 3. Methodology

An International Expert Group (IEG) on Major Sporting Events Security was formed in February 2020 during a closed-door meeting at the UN Headquarters in New York. Over 160 participants from security and law-enforcement agencies, international and regional sports federations, as well as private companies and technology entities involved in the security of, or with a direct interest in MSEs, as well as representatives from 80 Member States attended. The IEG is composed of a multisectoral community of experts and Member States that had either hosted or are planning to host an MSE. The consultation process for the drafting of the Guide was officially launched online during March 2020. Members of the IEG participated in five task groups: Background, Legal and Institutional Frameworks, Stakeholder Cooperation, the System and Deliverables (planning tools). Each task group was composed of a chair, a coordinator/drafter, and eight to ten expert members. The task groups engaged in regular online (due to COVID-19) consultation meetings with implementing partners, operational partners, the coordination team, and the project coordinator.

A common approach to collect and analyse information was promoted, and, as a first step information was collected through six different questionnaires which generated 77 responses, on relevant information, examples of best practices and lessons learned on the topics addressed in the Guide. Additionally, 17 video conferences with representatives from leading governmental agencies and members of local organizing committees responsible for MSE security, the private sector, international sports federations such as UEFA, FIFA, ICC and others were conducted. Informal conversations furthermore served to uncover new topics of interest that may have been overlooked by previous consultations and research. An expert group meeting in July 2020 regrouped over 200 participants to discuss the impact of COVID-19 on the security of MSEs. During discussions, participants focused on current and future challenges and threats, with an emphasis on the short-term and long-term impact of COVID-19 on security preparations, management and the hosting of MSEs.

To further explore critical aspects of MSE security planning, desk research was also conducted. This included the aggregation of useful instruments and the collection of past bidding documents, hosting and security guidelines as well as a review of reports and documents. A dataset on 23 past and upcoming MSEs was developed which enabled stakeholders to select case studies of particular relevance to the Guide. Based on this dataset, UNOCT disseminated a questionnaire to Member States[15] with significant experience and expertise in the area of organizing and hosting MSEs, with particular attention to security aspects, based on experience from countries in Europe, Asia, Africa, and the Americas.

The empirical basis for the Guide is the result of qualitative research, including responses to questionnaires, semi-structured interviews and informal conversations, and desk research. A validation process was undertaken by sharing the final content of the Guide with relevant experts and representatives from the Member States, and requesting their feedback.

## 4. Approach

The Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies promotes an integrated, inclusive, scalable, accountable, sustainable, interoperable and ethical approach to the preparation, organization and follow-up of MSEs, with the final aim of ensuring safe and secure environments for all participants and stakeholders involved, while at the same time providing a welcoming environment for spectators.

This approach can be detailed as follows:

- **Integrated:** As defined by the Council of Europe's Saint-Denis Convention, an integrated approach, hereinafter also referred to as the "3S approach" is based on the "recognition that, irrespective of their primary purpose, safety, security and service measures…invariably overlap, are interrelated in terms of impact, need to be balanced and cannot be designed or implemented in isolation."[16]
- **Inclusive:** Supports the notion of implementing a multi-agency, multi-sectoral and multi-level engagement, by the inclusion and pro-active participation of all stakeholders involved in the different elements of safety and security, including measures to attract and treat equally all groups of society to an MSE, notably the most vulnerable groups including women, children, elderly people, disabled persons, national minorities, refugees and asylum seekers.

[15] Algeria, Angola, Brazil, Canada, China, Colombia, Egypt, Mexico, Germany, Ghana, India, Indonesia, Japan, Morocco, Panama, the Philippines, Republic of Korea, Senegal, South Africa, Sri Lanka, United Kingdom of Great Britain and Northern Ireland, and the United States of America.

[16] A multi-agency integrated approach;see https://www.coe.int/en/web/sport/a-multi-agency-integrated-approach.

- **Scalable:** Indicates that the approach set out in the Guide can be applied to any MSE, regardless of the size of the event, and that planning can be adapted rapidly for the eventual success of the event.
- **Accountable:** Means that there should be a clear line of accountability for the planning and delivery of the security plan.
- **Sustainable:** Supports the notion that decisions must have a long-term impact, maintain relevance over time and always take into account environmental, societal and economic considerations.
- **Interoperable:** Ensures that security plans, policies, communications, and human resources are synchronized to work together during the MSE.
- **Ethical:** Alongside the above approaches, the inextricable link between security and human rights is emphasized throughout this Guide, calling for respect for universal and fundamental ethical principles, as enshrined in the main international conventions on the protection of human rights.

# II. POLITICAL, ECONOMIC AND SOCIAL DIMENSIONS OF MAJOR SPORTING EVENTS

Major Sporting Events are large undertakings for Host Authorities and the motivations underlying the organization of a sporting event of such international magnitude usually go beyond the world of sports and enter the world of international relations.

Despite the objective difficulty in accurately evaluating the real economic costs of hosting an MSE, and regardless of the fact that in recent years many citizens have come to look at MSEs with an increasingly sceptical eye, it is undeniable that MSEs have repeatedly obtained international, and at times even geopolitical relevance. MSEs also offer opportunities to promote positive change within a hosting country as well as for the international community at large. MSEs have social, political and diplomatic dimensions, offering an opportunity to strengthen international dialogue.

MSEs provide Host Authorities with an excellent opportunity to display their cultural heritage to the world and to showcase the venue city as a desirable place to live, work, do business and, last but not least, to practise sport.

The decision to hold an MSE is also a reputational issue, and decision-makers should be well aware that careful security planning plays a central role in this regard. On the one hand, a positive security experience can allow the host country or city to earn prestige from the event and to showcase it as a global destination for tourism and business. On the other hand, if a serious security incident takes place, it can be the defining moment of a particular MSE, with potentially very harmful effects, notably on tourism.

MSEs are often unique catalysts for Host Authorities to modernize infrastructure, locally or across the country, to align legislation to international standards and norms, and to promote human development and the concept “we are one world”. MSEs can also yield evidence of progress made towards the UN’s Sustainable Development Goals (SDGs) and to become part of the voluntary reporting framework used by countries.

With regard to socio-economic impact, the organization of an MSE constitutes a multidimensional window of opportunity, with potential for short-, medium- and long-term benefits.

- In the short term, during the event, the economic spinoffs can be highly significant as a community may see visible and immediate benefits, including growth in tourism, temporary employement and economic activity, despite the high costs of delivering an MSE.[17]
- In the medium term, the construction or modernization of existing infrastructure can constitute an added value for the community, including urban regeneration, new sporting facilities and sports development.[18]
- The successful organization and hosting of an MSE can also project an image of accomplishment, showing the Host Authority's capacity to work collectively towards common goals that positively impact the tourism sector, economic and trade performance, and international relations.
- In the long term, the Host Authority accumulates know-how that can be put to use in other events.

Regarding the economic dimension of MSEs, most studies show that organizing an MSE more often than not has ended in a net short-term financial loss for the Host Authority.[19] This negative outcome seems to be the result of high direct costs and limited, measurable returns.[20] One of the few exceptions to this trend appears to be the 1992 Summer Olympics held in Barcelona.[21]

[17] For example, the Summer Olympics Los Angeles 1984, FIFA Football World Cups. See http://www.pages.drexel.edu/~rosenl/sports%20Folder/Economic%20Impact%20of%20Olympics%20PWC.pdf .

[18] For example, the Summer Olympics in Barcelona, Greece, or Rio de Janeiro, or UEFA EURO 2004; see https://www.olympic.org/news/athens-infrastructure-boosted-by-olympic-games-2004 .

[19] See Cornelissen 2009; Peters, Matheson and Szymanski 2014; Pillay and Bass 2008). Zimbalist (2015, p. 40-43) reviews 19 academic studies of hosting the Olympics and the World Cup but could not find a single case that showed consistently positive economic effects. In: Theiner, Patrick. "Faster, Higher, Stronger? The Political Effects of Sports Mega-Events". Baltimore: ISA Annual Convention Paper, 2017.

[20] In their review of more than 50 years of Olympic host authorities, Flyvbjerg and Stewart (2012) found that the Games overrun their budget in every single case and incurred an average of 179 per cent of their anticipated costs in real terms. The authors concluded that hosting the Olympics is a risky financially gamble. Flyvbjerg, Bent, and Allison Stewart. "Olympic Proportions: Cost and Cost Overrun at the Olympics 1960-2012." *SSRN Journal. Elsevier BV* (doi:10.2139/ssrn.2238053.); cf. also Patrick Theiner, "Faster, Higher, Stronger? The Political Effects of Sports Mega-Events", Baltimore: ISA Annual Convention Paper, 2017, p. 2.

[21] Since the early 1990s, achieving the "Barcelona effect" has been a key objective of organising committees of international MSEs. This concept actually has its origins in the positive economic return of US$ 225 million of the 1984 Los Angeles Olympic Games. Such a positive outcome also resulted from the Barcelona Olympics in

The appetite to host MSEs has varied from region to region over time. Since the turn of the twenty-first century, there has been a shift of opportunities to organize and host MSEs to regions other than the traditional ones. This "democratization" of MSEs has taken time, but by now all continents have held at least one MSE. The Asian continent has been particularly active in hosting MSEs since the 1980s - most notably Japan, the Republic of Korea and China. Latin America has hosted MSEs intermittently since the 1930s. Most recently, Brazil hosted the FIFA World Cup™ and the Olympics, in 2014 and 2016 respectively. Meanwhile, the African continent has hosted the Rugby World Cup in South Africa in 1995, the FIFA World Cup™ in South Africa in 2010 and will host the Youth Olympics in Senegal in 2026.

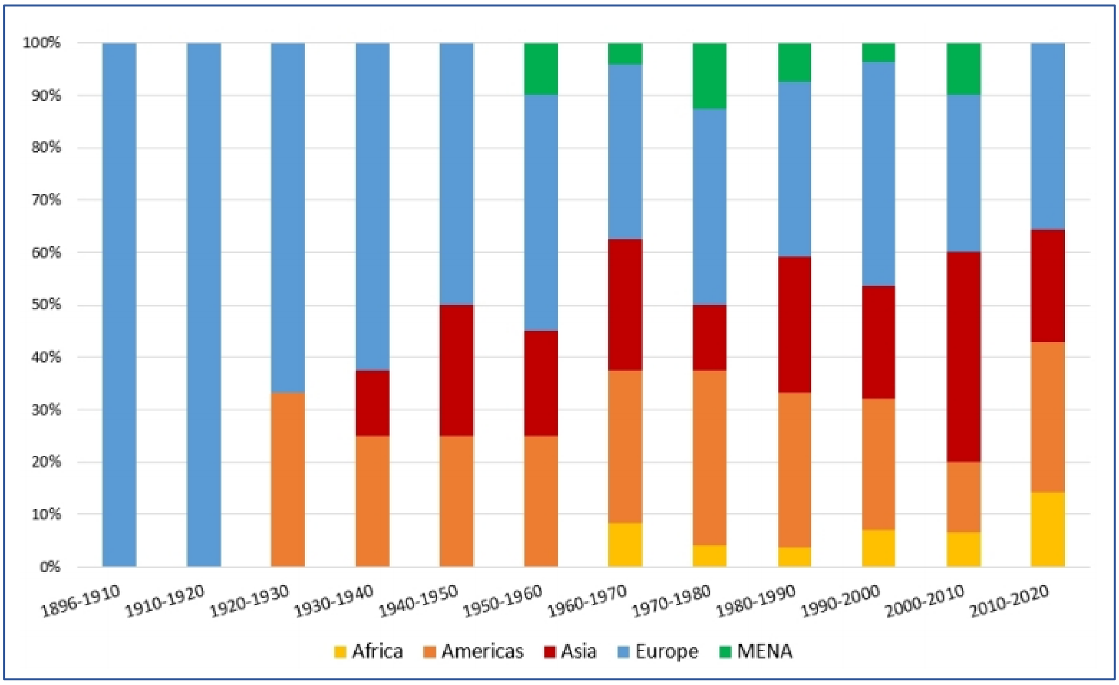


*Figure 1: MSEs organized by region 1969-2017*[22]

1992. This indicates that it is indeed possible to achieve tangible (and measurable) benefits if an event is properly planned from the outset.

[22] Patrick Theiner, op. cit., p. 20.

# III. FOUNDATIONS OF SECURITY AT MAJOR SPORTING EVENTS

There are certain elements that are essential when it comes to planning, delivering and executing the security elements of an MSE. Whilst the focus and balance of these necessities might change from one MSE to the next, the elements described below are indispensable for successful security operations.

## 1. Leadership and Vision

MSE security preparation, planning and delivery is a balancing act for the leadership. The complexity of the event and the number of stakeholders involved accentuates the need for effective leadership. A single leader or a very small team should be accountable to decide, plan and prepare, while different teams deliver on security, to maximize the effectiveness of the multitude of security agencies involved. It can be challenging to manage the sometimes-divergent expectations of the host authority, the local organizing committee and private-sector partners.

Experience has shown that two contrasting leadership styles – relationship-oriented leadership[23] and task-oriented leadership[24] - exist. Both styles are equally valid, depending on the situation. It is also important to have the right set of managerial skills, as MSEs are projects that have to be carefully planned and diligently executed.

The key to success is selecting a leader (or small leadership team) with proven skills in managing complex projects and building relationships, someone who has the trust of their colleagues and partners. Building trust is one of the most important competencies required for a leader when challenges to jurisdictional authority, command and control of resources and lines of reporting in a multiagency and multitasking process threaten the success of the MSE. The leader must earn the trust of those they work with. This trust, consisting of a combination of capability, competence and concern, is the foundation that all other team values ought to be built on.

[23] This style is used in diplomacy to strengthen relations with strategic partners and to show concern for the needs of planners who are obliged to carry out the security planning mandate.

[24] This style places the focus on motivating task performance by setting goals, ensuring proper supervision, and making sure planning remains on track.

It is essential to realize that effective leadership refers not only to competence but also to ethical behaviour. Leaders have the responsibility to ensure high standards of moral conduct that can set the tone for the entire organization. An MSE leader must always respect the principles of legality and proportionality, as well as respect the values of diversity and inclusiveness, gender and racial equality, and demonstrate integrity. Ethical leadership includes leading in a manner that respects the rights and dignity of others. The importance of this is amplified in an operation involving multinational partners. When organizing an MSE, it is vital that leaders are selected based on a proven track record of ethical and moral behaviour.

Right from the exploratory phase moving into the delivery phase of an MSE, it is essential for the central organizing entity to define the vision of what the event should be, what should it bring to the country and to the local community as a whole in terms of quality of life, safety and security, as well as in terms of the image and legacy it seeks to project. The vision must be determined from the outset and kept in mind from the planning stage until final delivery. This vision should be supported by a clear mission statement, a division of responsibilities and a realistic allocation of tasks.

**Recommendations:**

**Leadership and vision**

- → Select leaders in charge of the security of MSEs based on a proven track record of ethical and moral behaviour.
- → Ensure that leaders in the security field act strictly within the law and that they are fully committed to the values of diversity, inclusiveness, gender and racial equality.
- → Include the security mission within the broader vision for the MSE and align security considerations to the MSE's core organizational values.

## 2. Coordination, Continuity, Cooperation, and Communication

This Guide strongly advocates the use of the concepts of *coordination, continuity, cooperation and communication* (the 4Cs) as essential success factors to be observed across all phases of the security preparations of an MSE. These factors may be described as follows:

- ***Coordination***

With regard to the security preparations of an MSE, coordination refers to the ability to establish an environment which supports a leadership structure with a coordinated chain of command that reflects the security vision for the MSE, executes the necessary preparatory steps towards the establishment of the MSE security system and delivers the event.

As a vastly complex, multisector and multi-agency undertaking, the success of an MSE will greatly depend on the existence of a loyal and collaborative spirit, thus attesting that sound and effective multi-agency consultation is at the heart of the security system and the operations of an MSE. This includes the seamless meshing of public and private security services.

**Recommendations:**

**Coordination**

→ Plan and manage the security process for an MSE by involving a wide range of national authorities (e.g. Ministries of Interior, Justice, Defence, Security, Foreign Affairs, Sport, Treasury, Planning, Transportation and Health) in the decision-making process.

→ Ensure that security coordination efforts reflect multi-level institutional arrangements in the hosting country (roles and responsibilities of national and local levels of Government in the security arena).

→ Include the business sector and civil society in security-related decision-making processes.

→ Ensure that security planning and management are supported by adequate legal and regulatory frameworks outlining, among others, clear and smooth procedures aimed at the identification of roles, timelines as well as hierarchical and reporting mechanisms.

→ Engage highly qualified staff to work on safety and security tasks and provide them with specialized training on the implications of handling an MSE. Staff from private security agencies, when recruited, should also undergo appropriate training.

→ Make interagency coordination efforts effective by establishing interoperable databases, communication and information-exchange systems.

- ***Continuity***

Continuity refers to the development and uninterrupted implementation of the overall mission and the related security concepts along all the stages of the exploratory phase, bidding, planning, organization and implementing of the MSE. Given the time lapse between the initial exploratory phase and the execution of the MSE (people in key positions and administrations might change before the event takes place), the element of continuity is crucial to protect steady progress and deliver the event in time. Continuity also ensures that the intended legacy can be achieved and thus guarantee that the MSE's positive record is preserved.

**Recommendations:**

**Continuity**

→ Plan for security (e.g. budgets, human resources) in a sustainable and realistic manner by minimizing risks of the time gap between planning and delivery, which affect the quality and extent of security.

→ Ensure that the security objectives are fully understood, endorsed and acted upon by all stakeholders throughout event planning and delivery, particularly in cases of personnel changes.

→ Establish mechanisms to continually evaluate the proper functioning of security systems and processes as well as their continued relevance in the face of a changing security environment, technological advances, institutional restructuring, etc.

- ***Cooperation***

Close cooperation with local and international, public and private partners and all other key stakeholders, including those in the health sector, must start at the very early planning stages and continue through to the post-event stage. This element is distinct from coordination since it implies a voluntary act of sharing information, proactive support, availability and knowledge as a means to bring about the event's success, rather than merely conforming to orders coming down an imposed chain of command.

**Recommendations:**

**Cooperation**

→ Promote an environment whereby all stakeholders with security-related responsibilities (e.g. transport, health, police and fire) share the same values and collaborative spirit, in line with the notion of joint participation in a multi-agency and multisectoral approach.

→ Encourage the voluntary and proactive sharing of knowledge and technical support between all stakeholders involved in security planning, organizing and delivery.

- ***Communication***

Communication plans and strategies are crucial to ensure success during all phases of an MSE. A diverse group of stakeholders must have a clear and common understanding, from the very early stages, of who should produce, disseminate and receive information and how communication should flow both vertically and horizontally among all those with a need to know.

**Recommendations:**

**Communication**

→ Develop and actively promote a comprehensive communication strategy accessible to all stakeholders performing security-related tasks in relation to the MSE, both from the public and the private sector.

→ Set up adequate infrastructure and information/communication technologies for the timely and secure exchange of operational information within participating agencies.

→ Implement a process of continuous consultation throughout the MSE event cycle to regularly integrate security-related feedback from all stakeholders.

## 3. Good Governance

In recent years, international development agencies have promoted the concept of "Good Governance". In 1996, the International Monetary Fund (IMF) Executive Board identified "promoting good governance in all its aspects, including ensuring the rule of law, improving the efficiency and accountability of the public sector, and tackling corruption as an essential element of a framework within which economies can prosper". [25]

The Good Governance concept was further developed by several UN agencies and programmes and introduced in diverse spheres of the United Nations. According to the UN High Commissioner for Human Rights,[26] the core elements of Good Governance include transparency, integrity, lawfulness, sound policy, participation, accountability, responsiveness,

[25] See https://www.imf.org/external/pubs/ft/exrp/govern/govern.pdf .

[26] United Nations Human Rights Office of the High Commissioner (UNOHCHR), and https://www.ohchr.org/EN/pages/home.aspx .

and the absence of corruption and wrongdoing. The key question that the Office of the High Commissioner for Human Rights asked was this: "Are the institutions of governance effectively guaranteeing the right to health, adequate housing, sufficient food, quality education, justice and personal security?"[27]

**Recommendations:**

**Good governance**

→ Ensure that principles underpinning "good governance" inform all phases of the security-related decision-making processes for an MSE.

→ Establish solid good-governance models and ensure their dissemination across the whole spectrum of agencies involved in security-related tasks for an MSE.

## 4. Proper Estimate of Security Costs

In light of the substantial size of security-related budgets and their impact on the overall budget of the event and the economy of the Host Authority, a careful and realistic estimate of costs is an essential step for a country to assess its capacity to host an MSE.

With the emergence of new and complex threats, security costs associated with organizing an MSE have steadily risen in recent years,[28] thus increasing the need to engage in meticulous budget calculations. A careful approach is required to assess the security costs of previous MSEs against the likely costs of the new event.

Due to the high security costs, it is recommended that security provisions be regarded as a worthwhile long-term investment, similar to investments in infrastructure development, and as more than an unavoidable one-time expenditure for the organizers and for the local community.

The estimation of security costs is intrinsically linked to two main factors:

[27] See https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

[28] Richard Giulianotti and Francisco Klauser (2010), 'Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda', *Journal of Sport & Social Issues* 34 (1); see https://www.researchgate.net/publication/43108443_Security_Governance_and_Sport_Mega-events_Toward_an_Interdisciplinary_Research_Agenda .

1. the level of security arrangements required to host the MSE associated with the scale of the event, as defined in the bidding documents; and
2. the level of investment available to allocate to the planning and operation of the security system.

A proper estimate of security costs in the very early stages of the planning process will explore the sustainability of growing expenditures and the capacity of a country or city to host the event and protect it from foreseeable threats and disruptions. In the normal course of action, costs are estimated properly for the first time during the bid evaluation in the exploratory phase, taking into account the following factors and considerations:

- Level of security arrangements required to host the MSE associated with the scale of the event, as defined in the bidding requirements.
- Initial estimates compared to the actual final security expenditures from past events of a similar nature in countries with similar characteristics and capacities.
- The amount of capital existing within the host economy to provide the security apparatus for hosting an MSE – i.e. do they have the equipment required already or does it need to be bought brand new?

The overall security budget of the MSE is agreed upon and managed at Host Government level. It covers the planning and operational costs incurred by law enforcement agencies to ensure an undisturbed and peaceful MSE. Several public funding streams are often needed to sustain security investments, depending on the host authorities political system and economic wealth.

The budget should account not only for the protection of venues hosting the competitions, but should also cover the costs for the protection of critical infrastructure and potential soft targets during the MSE, including those located in surrounding areas such as public venues, fan zones, public viewing areas, squares, traffic and evacuation routes, and means of public transport.[29]

In this sense, private security companies are an important budget line. Costs calculations for these services must include recruitment, training, uniforms, equipment, accommodation and transport.

[29] Security of the spectacle – The EU's guidelines for security at major events (2011); see https://www.statewatch.org/analyses/no-207-major-events-public-order.pdf .

## Recommendations

### Proper Estimate of Security Costs

→ Carry out an initial estimate of security costs as early as possible during the event planning process in light of an assessment of the capacity of a country/city to host the event and protect it from foreseeable threats and disruptions.

→ Account for costs involved in the protection not only of venues hosting the competition but also enabling critical infrastructure (e.g. electricity distribution networks) and potential soft targets surrounding the competition area (e.g. crowded bars where fans may gather).

→ Provide for sufficient budget contingencies to address change variances to the original planning assumptions.

→ If resort to private security firms is envisaged, budget costs for recruitment, training uniforms, equipment, accommodation and transport purposes.

→ Frame security costs as a medium- and long-term investments for the benefit of the community as opposed to expenses solely needed to secure a one-time event.

# IV. SECURITY CONSIDERATIONS BEFORE AND DURING THE BIDDING PROCESS

For any MSE, the bidding process is of critical importance, as hosting an event and compiling a competitive bid tends to be a demanding and expensive undertaking. An in-depth reflection on the security challenges, opportunities and cost implications of hosting an MSE should, therefore, occur before embarking on the bidding process. Once the decision to bid for an MSE has been taken, security conditions ought to be considered of paramount importance while consolidating the bidding document since these are essential elements in the evaluation process undertaken by the relevant international sports federation.

## 1. The Exploratory Phase

This phase starts when the international sports federation (ISF) publishes its bidding requirements, comprising the specifications of the MSE, demands made of the host and outlining specific timelines. The extent of work and the number of resources required at this stage very much depend on the size of the MSE.

A thorough analysis of the Bid requirements, including the technical security requirements, should be conducted already in the exploratory phase to determine what resources are needed and whether they can be made available. Therefore, repeated security risk assessments need to be conducted over time as the event draws nearer. From the moment of considering a Bid to the delivery of an event, between 8 and 13 years could pass,[30] meaning that the context in which the event is to take place, and its security conditions, are likely to change. Geopolitical and domestic issues can dramatically change the security and economic landscape surrounding an MSE. Drone technology, new cyber vulnerabilities, as discussed in this Guide, and regional epidemics or a global pandemic are examples of new security threats that have emerged in

[30] Olympic Games – For the 2020 Tokyo Olympic Games the opening bids were made in 2011 with the decision made in 2013, therefore giving the host seven years to prepare for the games. In the case of the FIFA World Cup, the bidding procedure for the 2022 event opened in January 2009. At that time, the organising committees had one month to register interest in hosting the MSE. 24 months later, in December 2010, the FIFA executive committee decided in a vote who would hold the event. This has given Qatar 12 years to prepare for the event. However, in 2010 the FIFA Executive Committee also voted on the hosting for the 2018 FIFA World Cup which gave the Russian Federation eight years to prepare for the event. In 2006, the International Cricket Council (ICC) awarded the 2011 event to Bangladesh, India and Pakistan five years ahead, the 2015 event in Australia and New Zealand nine years ahead and the 2019 event in England and Wales 13 years ahead. In the case of the Rugby World Cup, the expression of interest phase gives one year to host authorities to signal that they would be interested in hosting the games. Two years later a decision will be made on where the World Cup will be held. This gives the host six years to prepare for the games.

recent years. These would not have been considered when some of the current MSEs were being initially explored and costs determined. Labour strife and equipment supply shortages or delays in delivery can also create rapid cost increases. Predictive analytics and artificial intelligence-based models should be incorporated where feasible for known eventualities. Sufficient budget contingencies must be included to address change variances to the original planning assumptions. Consideration could also be given to establishing partnerships and/or sponsorships with stakeholders concerned about new or emerging threats and risks.

Alongside these initial considerations leading to the decision to submit a Bid for an MSE, an essential aspect must be addressed as soon as possible: the specific location or venues where the MSE will take place. Only by understanding and taking into due consideration the concrete specific cultural, social, economic and other characteristics of the place where the MSE will be held, will it be possible to identify and adopt the most suitable, proportionate and effective measures for successful security operations. Law-enforcement agencies should provide input at an early stage when it comes to choosing venue locations. Crime hot spot and trend analyses and neighbouring high-risk communities may influence site selection. Conversely, neighbourhood (re-)gentrification may be part of the legacy plan.

If the evaluation outcome of this stage is positive, a level-of-service concept should be developed that clearly defines the division of responsibilities and the respective security costs.

## 2. The Bidding Phase

Depending on the MSE, the bidding process normally starts a year or two before the selection of the Host Authority, when the ISF publishes the process and timeline to bid.

Drafting the Bid is a very complex undertaking. It is normally led by a Technical Bidding Team composed of representatives of relevant government sectors, e.g., Ministries of Sports and Home Affairs, relevant sports federations or associations, local authorities and representatives from the business sector and civil society – persons with a blend of major sporting event experience and high-level business skills.

It is recommended that the Technical Bidding Team establish from an early stage effective working relations with international police organizations such as the International Criminal Police Organization (INTERPOL) and regional bodies such as the Inter-ASEAN Police (ASEANAPOL), the African Police Cooperation Organization (AFRIPOL), the European

Union Agency for Law Enforcement Cooperation (EUROPOL), the Police Community of the Americas (AMERIPOL), the General Secretariat of the Cooperation Council for the Arab States of the Gulf (GCCPOL) and the Arab Interior Ministers' Council (AIMC), depending on the geographical location of the MSE.

A Bid document will normally include, under the technical requirements, information on the security components of the MSE, including tangible evidence of the ability to deliver a secure event, elements relating to the expected security legacy, an estimation of the security costs and their sustainability. These aspects are expected to instil the ISF with confidence that the desired outcomes of the MSE can be realized.

The bidding phase is characterized by a series of visits of the ISF's event specialists, who form the Bid's Inspection Teams, which interact with local/national government authorities. Once the Bid is formalized, the members of the ISF conduct a voting session to confer the rights to host the event to the successful bidding country.

When it comes to the assessment of that security element of the Bid document, the ISF's evaluation committees should pay particular attention to:

- The existence of a robust regulatory framework upon which to build proposed security planning for the MSE;
- Having a clear allocation of funds devoted to security operations;
- Resilience and responsiveness in the case of terrorist incidents and overall capacity to respond quickly to threats or attacks;
- Genuine concern for the legacy of security.

**Recommendations**

**Security considerations before and during the bidding process**

→ Conduct security-related assessments (challenges, threats, opportunities, cost implications) right from the exploratory stage, and foresee the holding of successive assessments over time as the event draws nearer, also in order to factor in new and emerging threats.

→ Where appropriate and feasible, leverage predictive analytics and artificial intelligence-based models as tools to sharpen the quality and precision of security-related assessments.

→ Choose venue locations as soon as possible, utilizing input and trend analyses by law-enforcement agencies at an early stage. Site selection should be influenced by factors such as, inter alia, crime hot spots and neighbouring high-risk communities.

→ Set up a Technical Bidding Team and develop effective working relations with international security and law-enforcement agencies such as the International Criminal Police Organization and regional bodies.

→ Carry out a thorough analysis of the technical security requirements outlined in the bidding document in order to determine levels of needed resources and anticipate levels of socio-economic disruption and impact to local communities in the lead up to, and during, the MSE.

→ Carry out an advance estimate of the type and level of military/ law enforcement resources that will be effectively available for deployment to the MSE (e.g. consider contingents that may have already been earmarked for International peacekeeping missions, impacting the number of resources deployable to the MSE).

# V. LEGAL AND INSTITUTIONAL FRAMEWORKS

The planning, organization and hosting of an MSE need to be executed within robust legal and institutional frameworks that facilitate the fulfilment of all security requirements, whilst also guaranteeing full respect for the human rights of athletes, spectators, staff and all those involved in preparing, building and servicing the required facilities. To this end, hosting nations must ensure that all relevant matters are covered by adequate legal and institutional frameworks.

This chapter provides a description and analysis of the existing legal mechanisms and instruments relevant to providing security for MSEs. It endeavours to leverage knowledge and awareness of the available legal resources to assist countries in overcoming the multiple legal challenges that the organization of an MSE may entail.

The need to have a proper legal framework in place when staging an MSE is paramount. While many situations occurring during MSEs may require immediate and determined action from officers and staff in charge of security, all such measures need to be undertaken in full compliance with the applicable legal standards in order to mitigate liability issues and to protect the interests of all the individuals and stakeholders involved in the organization of an MSE. In addition, international cooperation may not be possible or smooth without the appropriate legal bases upon which to engage foreign countries or international organizations, including enabling timely information exchange. For instance, during the organization of a recent FIFA World Cup™ events, the organizing authorities prevented several violent or dangerous foreign fans from entering the country. This successful action was possible thanks to the conclusion of a mutual assistance agreement with a country which is well known for the bad behaviour of some of its fans (hooligans) who pose a threat to peace and security at the MSE.

Covering all the legal aspects relevant to the planning, organization and implementation of a successful MSE requires knowledge of the existing international and national mechanisms and instruments and a sound understanding of their implementation and impact. In particular, international standards provide key elements that an adequate strategy aimed at securing an MSE should include:

- Standards and requirements to prevent and counter criminal threats;

- Solid legal and institutional bases aimed at facilitating cooperation and timely information exchange, often at the international level, between different agencies involved in the security process;
- Solid legal provisions to ensure the protection of human rights; and
- Basic principles regulating public-private partnerships in relation to security matters.

## 1. International Legal and Institutional Frameworks

Since MSEs are intrinsically multinational and may attract sophisticated professional criminals operating transnationally, it will be essential to assess relevant international standards when looking at security considerations.

The international legal framework relevant to security in MSEs is composed of several heterogeneous instruments. Some of them were specifically designed to bolster security in MSEs, e.g., the Council of Europe Convention on an Integrated Safety, Security and Service Approach at Football Matches and Other Sports Events (hereinafter cited as "the Saint-Denis Convention") and the Council of Europe (CoE) Recommendation of the Standing Committee on Safety, Security and Service at Football Matches and Other Sports Events.

Other instruments were not specifically created to support the security of MSEs but are crucial towards this end since they contribute to the overall protection of the wider community and of the multitude of vulnerable targets which could be attacked in the course of an MSE. For instance, the 2006 United Nations Global Counter-Terrorism Strategy (adopted in General Assembly resolution 60/288; see document A/RES/60/288);[31] or Security Council resolution 2341 (2017)[32] on the protection of critical infrastructure against terrorist acts, Security Council resolution 2396 (2017) addressing soft targets and the Security Council's Guiding Principles on Foreign Terrorist Fighters, and the 2018 Addendum to the 2015 Madrid Guiding Principles, provide further guidance on protecting critical infrastructure, vulnerable or soft targets as well as tourist sites, as do the Council of Europe Convention on the Prevention of Terrorism and the Council of Europe Convention on Cybercrime.

[31] See The United Nations Global Counter-Terrorism Strategy, A/RES/60/288 .

[32] See UN Security Council resolution 2341 (2017) .

The following subsections provide an overview of the key issues addressed by the international legal framework in the field of MSEs security, namely, 1) Terrorism and other criminal threats; 2) MSEs' security planning and management; 3) Respect for human rights; 4) Data protection and new technologies; and 5) Unified approach to secure MSEs.

## 1.1 Terrorism and other Criminal Threats

There are several threats that organizers and security planners of an MSE need to assess and prepare for in advance – for example, terrorist attacks on critical infrastructure, offences against public order (such as hooliganism), organized crime, corruption and cyberattacks. Policymakers of an MSE hosting country are advised to implement the various international instruments and tools aimed at preventing and combating criminal conduct.

| UNODC Counter-Terrorism Technical Assistance Programme |
|---|
| The Terrorism Prevention Branch (TPB) of UNODC is the key United Nations entity providing legal counter-terrorism technical assistance to the Member States.<br><br>As mandated by the United Nations General Assembly, TPB works to assist the Member States, upon request, with the ratification, legislative incorporation, and implementation of the universal legal framework against terrorism<br>*Source:* https://www.unodc.org/unodc/en/terrorism/index.html |

### *a. Terrorist Attacks*

Acts of terrorism are widely considered to be the most flagrant threat to the organization of an MSE. As one group of authors put it:

> Sporting events are considered part of a nation's critical infrastructure and key assets. The major goal of terrorist activity is to destroy or incapacitate critical infrastructure and key resources, cause mass fatalities, weaken the economy, and damage the nation's morale and confidence.[33]

Terrorist organizations frequently seek maximum publicity, which is one reason why MSEs can become especially attractive targets to them.

[33] Hall, Stacey A., et al. *Security Management for Sports and Special Events: An Interagency Approach to Creating Safe Facilities*. Human Kinetics 1, 2012.

There is no international legal instrument specifically devoted to combating terrorism in the context of an MSE. However, since the 1960s the international community has adopted, both at the regional and international levels, a series of resolutions, treaties and strategies on the prevention and suppression of international terrorism.

### *b. Breaches against Public Order and other Anti-social Behaviour*

MSEs in general, and in particular football competitions, regularly attract hooliganism, violence from rival fan groups, riots, racist behaviour, and other situations disrupting public order. From a legal perspective, this presents considerable challenges for the authorities in charge of the security of an MSE as they need to safeguard the health and well-being of all spectators, athletes and other individuals participating in an MSE while also preserving a pleasant atmosphere that makes sports events enjoyable and welcoming for everyone.

For more than three decades, the Council of Europe has played a crucial role in the internationalization of common standards in this field. Following the tragedy that took place at the 1985 European Cup Final in Brussels, where 39 spectators were killed during a stampede, the CoE adopted the European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches (1985).[34] The aim of the 1985 Convention is to prevent and control violence and misbehaviour, as well as to ensure spectator safety during sports events.

To better attain the above-mentioned objective of safeguarding participants’ health while preserving a pleasant atmosphere, in 2015 the CoE elaborated new instruments building upon the 1985 Convention. In 2015, the CoE Standing Committee of the Convention on Spectator Violence[35] issued Recommendation Rec (2015) on Safety, Security and Service at Football Matches and Other Sports Events.[36] Revised in 2019 and adopted in 2020, this instrument consolidates and updates all 26 recommendations adopted by the Standing Committee over the previous 30 years. Crucially, it assists States in the interpretation and implementation of that 1985 Convention and the new the CoE Saint-Denis Convention (2016),[37] by including specific guidance on recommended best practices.

[34] See CoE Treaty Series - No 120 .

[35] See Standing Committee of the Convention on Spectator Violence .

[36] See Recommendation Rec (2015) 1 of the Standing Committee .

[37] See CoE Saint-Denis Convention .

**The Saint-Denis Convention**

The Council of Europe Convention on an Integrated Safety, Security and Service Approach at Football Matches and Other Sports Events was opened for signature on 3 July 2016. The Convention is the only international binding instrument to establish an integrated approach, based on safety, security, and service. It provides measures based on the highest safety, security and service standards developed in Europe. According to its Article 1, states may apply the provisions of the Convention to any other sport, including non-professional matches.

*Source*: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680666d0b

The Saint-Denis Convention stresses the overlapping and interrelated character of these three concepts at MSEs, and the consequent need to balance their implementation. To this end, it suggests strong measures regarding cooperation between all public and private stakeholders involved in the planning, organization and implementation of an MSE. The role and actions of each agency need to be coordinated, need to be complementary and proportionate, and should be implemented as part of a comprehensive safety, security and service strategy. The Recommendation (2015) of the CoE Standing Committee Convention on Spectator Violence[38] supports the Saint-Denis Convention and provides important guidelines towards its effective implementation.

### c. *Organized Crime*

There are several ways in which organized crime can affect MSEs, such as money laundering, manipulation of sports competitions, cybercrime, drug and arms trafficking, "hit-man" services, intimidation, trafficking in human beings for labour or sexual exploitation, violent attacks by criminal gangs composed by groups of fans or hooligans, as well as criminal organizations encroaching upon groups of fans or hooligans from another country. In addition, organized criminal networks may infiltrate the process of supplying materials that are instrumental for the construction and functioning of the infrastructure underpinning an MSE, for example, by injecting counterfeit or sub-standard components. Several cases have been reported concerning irregularities in the construction of stadiums and the purchase of security material during the organisation of MSEs, such as the FIFA World Cup™:

[38] The Recommendation (2015) of the CoE Standing Committee Convention on Spectator Violence, as revised in 2019 and adopted in 2020: https://www.coe.int/fr/web/sport/recommendation-2015-1.

- There were cases reported where drug lords in Latin America owned major football teams, using them to launder crime proceeds and fuel other criminal industries;[39]
- There are numerous examples of sports events being organised for the very purpose of laundering money, e.g., friendly matches; [40]
- Manipulation of sports competitions (“match-fixing”);[41]
- Several fans and hooligans are members of dangerous criminal gangs, dedicated to a wide array of criminal activities, such as drug and arms trafficking, “hit-man” services, intimidation, violent attacks, etc.[42] These activities may not necessarily take place during the actual competitions in an MSE; however, given the profiles of these types of hooligans, their mere presence in an MSEs may represent a tangible threat.

A key international instrument to consider while preparing for an MSE is the United Nations Convention against Transnational Organized Crime (UNTOC).[43] In particular, UNTOC requires that State Parties:

- Establish as criminal offences conduct that is instrumental to the activities of criminal organizations, notably: participation in an organized criminal group, corruption, laundering of proceeds of crime and obstruction of justice;
- Develop adequate investigative tools such as special investigative techniques (electronic or other forms of surveillance, undercover operations, etc.). Such measures need to be subject to legislative safeguards to protect human rights;
- Establish witness protection schemes and incentives for cooperating offenders; and
- Establish legal bases and channels to facilitate international law enforcement and judicial cooperation (e.g. for extradition, the exchange of criminal evidence, the confiscation of proceeds of crime).

### *d. Cyberattacks*

It is difficult to imagine the organization of an MSE without relying on computer technology, as almost every facet of organization is affected by the working of computers and networking technology (see Chapter VII on the Security Planning, section Operations Plans). Regrettably,

[39]See https://es.insightcrime.org/noticias/analisis/10-formas-futbol-crimen-organizado-mezclan-latinoamerica/ .
[40] Idem.
[41]See https://www.coe.int/en/web/sport/manipulation-of-sports-competitions .
[42] Idem.
[43] See United Nations Convention against Transnational Organised Crime (UNTOC) .

most of the advantages in terms of interconnectivity that information technology brings come at a cost. Uncontrolled and unregulated developments in this field have created vulnerabilities that can be exploited by malicious actors. As a result, mitigating the impact of cyberattacks has become a central concern when it comes to ensuring the security of an MSE.[44]

The Senior Executive Team in charge of organizing an MSE, including government agencies, organizing committees and private-sector partners, need to be prepared to deal with cyberattacks and to understand cybersecurity challenges.[45]

In a nutshell, there are three key aspects of cyber risks:[46]

**Operational**: The risk that a cyberattack takes down the core operations system of a unit, agency or entity in charge of security, thwarting its functioning or even totally preventing the operating system's ability to accomplish its tasks. Event organizers could find themselves in serious trouble when trying to secure an MSE, particularly with the advent of the Internet of Things (IoT) which links up multiple industrial devices, from stadium lights to alarm systems.[47]

- **Legal and litigation risk**: When a cyberattack occurs, organizers in charge of security may be held liable by third-party individuals that have been affected by the attack. There are numerous examples of private companies that have been sued by their clients following a cyberattack because the corporate security system was judged to be inadequate, and the response to the attack was held to be late or not effective. In the context of an MSE, organizers could be liable for losing privacy-related information about their security staff, creating a wide array of problems that could result in liability lawsuits.
- **Reputational risk**: Any type of successful cyberattack can cause significant reputational damage to the image of the organizers of an MSE.

[44] Wells, D. et al (2016). "Challenges priorities and policies: mapping the research requirements of cybercrime and cyberterrorism stakeholders"; in: *Combatting cybercrime and cyberterrorism: challenges, trends and priorities.* B. Akhgar and B. Brester (eds.) Cham: Springer, 2016, pp.39-52.

[45] DiChristopher, Tom, 'Execs: we´re not responsible for cybersecurity'. See https://www.cnbc.com/2016/04/01/many-executives-say-theyre-not-responsible-for-cybersecurity-survey.html .

[46] McQuitty, Jake, David Cook, "Cyber Security: the Reputational, enforcement and litigation risks". See https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Litigation_Support/lawyer-article-cybersecurity .

[47] Matt Burgess, "What is the Internet of Things? WIRED explains". See https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot .

At the same time, given the rapid evolution of information technology, it is also essential that organizers of an MSE remain ahead of the curve when it comes to cyber-risk mitigation, both to avoid operational loss of control and to prevent liability lawsuits. To this end, governmental agencies, host committees and private-sector partners should adopt an effective cybersecurity framework, based on existing instruments, such as:

- The NIST Framework for Improving Critical Infrastructure Cybersecurity.[48] Elaborated by the US National Institute of Standards and Technology (NIST), this framework recommends considering cybersecurity risks as part of the organization's overall risk-management processes. While the document was developed to improve cybersecurity risk management for critical infrastructure, the framework can also be used in any sector or community, including MSEs; and
- ISO/IEC Security Control Standards.[49] The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) elaborated this framework aimed at managing information risk effectively.

### *e. Health-related Events*

Organizing authorities also need to consider health-related threats, for instance, communicable diseases or malicious attacks using chemical, biological, radiological and nuclear (CBRN) substances by terrorist and criminal organizations for extortion and blackmail. Given the fact that MSEs are mass spectator events, the concentrated presence of thousands of people poses both natural as well as man-made health risks. Terrorists and criminals may use any means to interfere with the successful conduct of an MSE, including by releasing pathogens. However, disease outbreaks might also occur without malicious intent; they can occur through acts of omission rather than commission when, for example, hygiene standards are not upheld.

Preparing public health systems to cope with this sort of threat is a complex and demanding task, which requires a thorough risk assessment and the creation of a flexible medical response mechanism. In 2015, WHO released an updated document on Public Health for Mass Gatherings: Key Considerations[50] covering the most relevant aspects related to health-related threats during the organization and implementation of major events. This WHO publication

[48] NIST Framework for Improving Critical Infrastructure Cybersecurity: see https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf .

[49] ISO/IEC Security Control Standards; see https://www.iso.org/isoiec-27001-information-security.html .

[50] See https://www.who.int/publications/i/item/public-health-for-mass-gatherings-key-considerations .

focuses on the main health-related issues at stake and provides a list of tools and resources to cope with contingencies (also see Section X on The Impact of COVID-19 in the Security of MSE). Notably, there are several international instruments, legal resources and standards that Host Authorities may wish to use to mitigate and prevent health-related threats during the organization of an MSE.

According to the WHO publication on Public Health for Mass Gatherings: Key Considerations,[51] authorities also need to address, inter alia, the following issues, which can be essential for an MSE:

- Public-health surveillance systems and situational awareness: authorities need to carefully assess the dimensions of the MSE in order to enhance surveillance, test laboratory and other monitoring systems (such as syndromic surveillance systems).
- Environmental health (food, water, air quality, etc.): improve hygiene training and detection.
- Public health awareness/understanding: Health promotion and education campaigns for enhancing public risk awareness.
- Communication and coordination at national and international levels: conduct exercises and training to assure proper functioning under emergency conditions, etc.
- Address potential CBRN risks (see subsection f below)

### *f. Chemical, Biological, Radiological and Nuclear (CBRN)*

Any solid strategy to prevent chemical, biological, radiological and nuclear (CBRN) incidents in the context of the preparation and organization of an MSE calls for a high level of cooperation and coordination at national, regional and international levels. As such, policymakers need to ensure that the applicable legal and institutional framework delineates in clear terms the responsibilities of all actors involved in this matter.

As mentioned before, MSEs can be subject to CBRN attacks by both criminal or terrorist organisations, whether for extortion or intimidation. Consequently, organizing authorities are called to conduct risk assessments and capacity-building activities to detect, alert and respond to a CBRN incident; developing CBRN preparedness and response systems; ensure flexible intersectoral cooperation at national, regional and international levels.

[51] See https://www.who.int/publications/i/item/public-health-for-mass-gatherings-key-considerations .

The provisions and mechanisms that States may need to use to counter CBRN threats are scattered over several legal instruments, which sometimes overlap. Hence, organizing authorities should consider tools and platforms and adapt their national legislation, regulations and policies accordingly.

### Tools and Platforms to counter CBRN threats

- ✓ UNODC publication on the International Legal Framework against CBRN Terrorism. The module is a technical assistance tool for training purposes that aims to familiarise policy- and decision-makers and counter-terrorism practitioners with the requirements of the relevant international legal instruments and assists legislative drafters and criminal justice officers with their effective implementation.
- ✓ WHO publication on *Public Health for Mass Gatherings: Key Considerations* includes a chapter on CBRN. From a health-security perspective, the document provides key considerations; guiding principles and best practices; and practical suggestions.
- ✓ The IAEA Publication on Nuclear Security System and Measures for Major Public Events. It describes nuclear security systems and measures that may need to be established or enforced to enhance overall security for the MSE.
- ✓ Governmental authorities may also rely on the UNICRI CBRN Risk Mitigation and Security Governance Programme. This programme seeks to foster an integrated response at the national level to mitigate CBRN risks. To this end, UNICRI proposed specific indicators to assess the functioning and preparedness of 1. Interagency coordination; 2. Operations communication; 3. Collaboration with non-governmental stakeholders; 4. Regional and international cooperation; 5. Planning; and, 6. National, regional and international standards.
- ✓ INTERPOL has a specialized CBRNE Unit for Radiological and Nuclear Terrorism; Bioterrorism; and Chemical and Explosive threats. The programme consists of three pillars: 1—intelligence analysis for police services; 2. Programmes preventing the illegal dispersal of CBRNE materials; 3. Responding to, and investigating, CBRNE threats and malicious incidents.

*Source*: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1546_web.pdf

Policymakers and other relevant authorities in charge of planning, organizing and implementing an MSE may use the opportunity as a catalyst to develop national CBRN risk-mitigation strategies that will be useful beyond the life of the MSE.

## 1.2 MSE Security Planning and Management

To address terrorist and other criminal threats in the context of an MSE, organizers need to set up, and effectively manage, a robust security apparatus (see Chapter VII on The Security Planning). From a legal perspective, a number of international instruments can provide useful tools to this end.

- **Governance: Government, Host Organizers and private-sector partners**

Public authorities (e.g., ministries, law enforcement agencies), ISFs (e.g., FIFA, UEFA, IOC, ICC) and Host Committees and private-sector partners (e.g., venue owners, private security, sponsors) need to work collaboratively to ensure the security of athletes, spectators and the general public. To achieve this objective, it is necessary to delineate responsibilities and roles clearly, including chains of command, put in place specific regulations on accountability, contingency plans and develop a fully-fledged outline of cooperation between them. In brief, the security planning apparatus needs to be built on a robust Good Governance model.

- **Human and Material Resources (Private Security and Procurement)**

For the purpose of upholding security, organizers of MSEs will have to invest substantially in both, human resources and material assets (see Chapter VII on The Security Planning, the section on Integrated Planning Process). International standards in this field have evolved during the past decades, requiring organizers to ensure that all competent personnel from both the public and private sectors are equipped and trained to fulfil their functions effectively (Saint-Denis Convention, Article 5.6).

Organizing authorities are increasingly turning to the services of private security providers and other professionals, particularly when it comes to stadiums and contiguous zones where safety and security are often entirely implemented by private companies as national police forces and military support units alone may not be in the position to adequately secure MSEs. In such cases, the tasks performed by the private entities ought to be monitored by national law enforcement agencies, which are usually in charge of certifying and approving the activities of these private security firms.

The task of upholding security at an MSE also requires a substantial amount of material resources, including technology, building material for infrastructure, vehicles, etc. It is essential for both public and private-sector organizers to have open and transparent procurement processes in place, accompanied by robust auditing and public scrutiny measures. Regrettably, during the past decades, there have been several cases of inefficiencies, corruption and misconduct in relation to purchases/procurement done in preparation of MSEs.

## 1.3 Respect for Human Rights

When introducing new legislation or amending existing laws to secure MSEs, (e.g. laws to counter terrorism and control hooliganism and fan aggression), Governments need to carefully evaluate the impact of legislative measures on human rights.

To combat potential terrorist threats at MSEs, authorities may limit certain rights, so long as restrictions comply with the conditions set out in international human rights law. In particular, any restrictions must be prescribed by law and must be proportionate to the pursuance of legitimate aims and should be non-discriminatory.[52] Temporary restrictions on certain human rights must correspond to the magnitude of the threat at hand, as required by the exigencies of the situation, and must be adequate to address the threat efficiently.

International organizations have also produced a number of standards devoted to fighting racial discrimination, xenophobia and related intolerance, phenomena which could manifest themselves in the course of an MSE. Although sports events can be great catalysts to build cohesion between people and countries, several such events have been marred by openly racist conduct. To underpin the principles enshrined in the UN International Convention on the Elimination of All Forms of Racial Discrimination (CERD),[53] sports organizations such as UEFA, FIFA and the IOC have produced several regulations and policies aimed at mitigating and preventing racism, racial discrimination, xenophobia and related forms of intolerance. Discrimination against women in sports also needs to be addressed. The UN Human Rights Council has raised concern in relation to sports regulations and practices that discriminate against women and girls on the basis of race, gender or any other ground of discrimination. It has called upon States to ensure that sporting associations and bodies implement policies and

[52] Human Rights Committee general comment No. 31 (2004) on the nature of the general legal obligation imposed on States Parties to the Covenant.

[53]See https://www.ohchr.org/en/professionalinterest/pages/cerd.aspx

practices in accordance with international human rights norms and standards.[54] The UN Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)[55] provides that States parties shall grant women the same opportunities as men to participate in sports.

Adherence to international human rights standards, including labour rights, is also crucial during the preparation of an MSE. Unfortunately, several past events have been associated with forced evictions of people for the construction of venues, high rates of accidents among workers, as well as migrant workers' exploitation and sweatshop labour conditions.[56] To mitigate those risks and rights violations, national authorities ought to refer to the International Labour Organization (ILO) Conventions and Recommendations[57], which establish solid labour standards, and the UN Guiding Principles on Business and Human Rights[58], which delineate in clear terms the obligations of employers to comply with human rights norms.

## 1.4 Data Protection and New Technologies

The acceleration in the enactment of data protection laws worldwide, and the existing commitment to privacy and data protection as fundamental rights in many countries around the globe are to be taken into consideration. International human rights law provides a clear universal framework[59] for the protection of the right to privacy. The right to data protection is also particularly relevant in the field of security in MSEs, as many new technologies or special investigative techniques have considerably increased law enforcement capabilities to gather and store data. In this regard, it is recommended that MSE hosting authorities comply with applicable regulations and standards, such as the the Convention on the protection of individuals with regard to the processing of personal data (also known as Convention 108[60] which is the sole international treaty on data protection open to accession to any country in the world with a complying legislation), European General Data Protection Regulation (GDPR)

[54] See document A/HRC/RES/40/5.

[55]See https://www.ohchr.org/EN/ProfessionalInterest/Pages/CEDAW.aspx .

[56] See https://www.sporthumanrights.org/en/resources/mega-sporting-event-lifecycle-embedding-human-rights-from-vision-to-legacy .

[57] For ILO Conventions, see http://www.ilo.org/global/standards/introduction-to-international-labour-standards/conventions-and-recommendations/lang--en/index.htm .

[58] See UN Guiding Principles on Business and Human Rights and https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf .

[59] See https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx .

[60] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

and Law enforcement Directive of the European Union.[61] International organizations dedicated to police cooperation have also developed tools to assist the law enforcement community, such as:

- INTERPOL's Data Protection Framework, regulating the exchange of police information to ensure it is in full compliance with Data Protection Standards. In addition, this organisation regularly introduces programs to familiarize national law enforcement agencies in the use of new technologies, such as Facial Recognition[62].
- The Europol Data Protection Function (DPF) regularly produces guidelines and suggests procedures to enhance police forces' capabilities to act in full compliance with Data Protection Standards.[63]

## 1.5 Unified Approach to Secure an MSE

The planning, organization and delivery of an MSE require that organizers ensure the smooth working of Inter-agency cooperation; public-private partnerships; strategic communication; and international cooperation.

States need to prepare their legal and institutional frameworks to enable the effective execution of these elements, which are at the heart of an integrated approach to secure an MSE. These components have been enshrined in several international instruments, strategy documents and guidelines. To effectively implement them within the context of the planning, organization and implementation of an MSE, Host Authorities should identify the gaps existing in their national legislation and fill them with the help of applicable international standards. In particular, these are:

- Saint-Denis Convention[64]: Article 4 on Domestic coordination arrangements; Article 5.6/7 on safety, security and service in sports stadiums [see Box]; Article 7 on Contingency and emergency planning; Article 8 on Engagement with supporters and local communities; Article 9.3 on Police strategies and operations; Article 11 on International Cooperation;

[61] See https://ec.europa.eu/info/law/law-topic/data-protection_es .

[62] See https://www.interpol.int/How-we-work/Forensics/Facial-Recognition .

[63] See https://www.europol.europa.eu/functions/data-protection-function-dpf .

[64] See https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680666d0b .

- Security Council resolution 2341 (2017) on Protection of Critical Infrastructure:[65] operative paragraphs 1 and 8 on the enhancement of international and regional cooperation to protect critical infrastructure, including regional connectivity projects and related cross-border infrastructure;
- United Nations Convention against Transnational Organized Crime (UNTOC)[66]: Article 13 on international cooperation for purposes of confiscation; Article 16 on extradition; Article 18 on mutual legal assistance; Article 19 on joint investigations; Article 26 on measures to enhance cooperation with law enforcement authorities; Article 27 on law enforcement cooperation; Article 28 on the collection, exchange and analysis of information on the nature of organized crime; and Article 29 on technical assistance; and
- CoE (2001) Convention on Cybercrime ("the Budapest Convention")[67]: Chapter II, Title 5 on the real-time collection of computer data; Chapter III on international cooperation.

## 2. Strengthening National Legal and Institutional Frameworks to Secure MSEs

Prior to embarking on the organization of an MSE, national policymakers should:

- Develop a clear understanding of impacts and implications of applicable national legal and institutional frameworks related to the organization of an MSE, including both international instruments and the specific rules and regulations of the sports organisation under whose auspices the event will be organized (FIFA, ICC, IOC, CAF, CONMEBOL, IAAF, FIBA, IOC, UEFA, etc.); and
- Undertake a "mapping exercise" of the applicable national legal frameworks to check what new legal and judicial powers, mechanisms or instruments may be needed in addition to the existing ones.

In particular, policymakers involved in security-related matters should conduct a careful assessment of the following:

[65] See https://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2341%282017%29&referer=/english/&Lang=E .

[66] See https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html .

[67] See https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 .

- Whether the necessary legal tools are in place to prevent and counter-terrorism and other criminal threats affecting the planning or execution of an MSE, e.g., violent incidents, hooliganism, discrimination and other hate crimes, organized crime, cyberattacks, etc.
- Whether adequate regulations are in place governing all the aspects that the security planning of an MSE requires, including the identification of human and material resources, and procurement issues; this includes laws covering all matters related to security management, such as regulations on the role and accountability of law enforcement agencies and private security companies, information management, health plans, etc.
- Whether the relevant national legislative and institutional frameworks provide effective measures and safeguards to guarantee respect for human rights within the context of an MSE.
- Whether the existing legal and institutional framework supports an integrated approach to the planning, organization and implementation of an MSE, enabling smooth inter-agency and international cooperation, timely information exchange and strategic communication.

Crucially, the above assessment should be carried out early in the planning phase, with sufficient time to allow amendments and modifications to national laws and regulations, if needed. It is of paramount importance that host nations are not only "operationally" prepared well in advance, but also "legally and institutionally" prepared. Broadly speaking, there are two methods that host nations can follow to adapt their legal and institutional frameworks to the multiple requirements that the planning, organization and implementation of an MSE require:

- Countries may introduce and/or amend existing pieces of legislation dealing with the various aspects of security-relevant for the planning and conduct of an MSE; or
- Countries may enact an overarching law specifically addressing a forthcoming MSE or sport security.

**Recommendations**

**International legal and institutional frameworks**

→ Undertake an early-stage, comprehensive review of the legal preparedness of the country to host the MSE, considering, in particular, the time needed for legislative/ regulatory overhauls to be enacted through the country's normative and bureaucratic processes.

→ In conducting the above-mentioned legal review, in particular, determine gaps and needs for reform in terms of a) whether the domestic legal framework is sufficiently equipped to prevent and counter-terrorism and other criminal conduct potentially affecting the organisation of an MSE; b) whether adequate regulations are in place governing security planning and management of an MSE; c) whether national legislative and institutional frameworks provide for effective measures and safeguards to comply with international human rights standards (e.g. legality, proportionality, non-discrimination).

→ Determine the extent to which legal enhancements should be introduced via legislation/ regulation explicitly focusing on the forthcoming MSE versus the adoption/amendment of generally applicable normative tools (e.g. criminal codes).

→ As part of the preparations for an MSE, consider priority ratification (where applicable) and/or implementation, of the following instruments:

- Universal (UN) Legal Instruments for the Prevention and Suppression of International Terrorism;
- UN Convention against Transnational Organized Crime and its Protocols;
- Council of Europe Convention on Cybercrime;
- United Nations Global Counter-Terrorism Strategy;
- Security Council resolution 2341 (2017) on protection of critical infrastructure against terrorist acts;
- Security Council resolution 2396 (2017) and the 2018 Addendum to the 2015 Madrid Guiding Principles (Foreign Terrorist Fighters);
- Council of Europe Recommendation Rec (2015) on Safety, Security and Service at Football Matches and Other Sports Events.
- Council of Europe Convention on an Integrated Safety, Security and Service Approach at Football Matches and Other Sports Events
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism
- Council of Europe Convention on the Prevention of Terrorism
- European Convention on the Suppression of Terrorism
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime
- European Convention on the Compensation of Victims of Violent Crimes
- Council of Europe Anti-Doping Convention

Council of Europe Convention on the Manipulation of Sports Competitions

# VI. STAKEHOLDER COOPERATION

International and multisectoral collaboration is essential to ensure that the planning of MSEs results in a secure environment for spectators, athletes, dignitaries, volunteers, support staff and journalists. Partnerships between Governments, law enforcement agencies, international and regional organizations, international, regional and national sports bodies, organizing committees, the business sector, civil society and local communities leverage the expertise and resources of all entities and provide complementary perspectives into various areas of event delivery.

The purpose of this chapter is to provide an overview of collaborative efforts as these relate to security planning. It outlines key considerations for Host Authorities, in particular the authority responsible for security. It also recommends the incorporation of the 10 principles set out in the UN Global Compact,[68] and the UN's Sustainable Development Goals (SDGs)[69] wherever pertinent and possible, working cooperatively with all stakeholders, including civil society organizations and community groups.

Every Host Authority can benefit from collaborative partnerships to assess risks, set-up a comprehensive strategy, define an efficient organizational structure, and identify, locate and make available resources to support the planning and the delivery of an effective security operation during an MSE.[70] To work together, these alliances must navigate the complex political, social, and economic environment to:

- Strengthen legal and institutional capacities to improve the understanding of existing laws and norms of behaviour (see the Chapter on Legal and Institutional Framework);
- Develop confidence-building measures to support stable and sustainable relationships;
- Improve cooperation mechanisms between key actors for better information and intelligence exchange, situational awareness, and coordination of response;
- Create conditions to facilitate the sharing of resources, both human, material and technological, among different countries; and

[68] See https://www.unglobalcompact.org/what-is-gc, and URL: https://www.unglobalcompact.org/what-is-gc/mission/principles .

[69] See https://www.un.org/sustainabledevelopment/sustainable-development-goals/ .

[70] Pisapia, G. 2017. *Major Sport Events Safety and Security Framework's Core Elements*. See https://www.researchgate.net/publication/333827474_Major_Sport_Events_Safety_and_Security_Framework's_Core_Elements .

- Strengthen mechanisms and procedures for crisis management.

## 1. Benefits and Challenges

There are many examples of the benefits generated from stakeholder cooperation in the bidding, planning and execution of security for MSEs. Engaging stakeholders from civil society, both public and private sectors, as well as international stakeholders in an inclusive interchange, can help share risk, add value, efficiency, and scope to the security template, and support the development of solutions that incorporate all the various perspectives and resources necessary to adequately address the challenge of contemporary MSE security.

These collaborations can also lead to much broader benefits at the local, national and international levels, in terms of:

- Improving engagement, transparency, and accountability, internationally and across sectors;
- Building resilience and improving the security ecosystem in the long-term;
- Strengthening formal and informal cooperation frameworks between countries;
- Expanding capacity for information and intelligence-sharing on potential threats;
- Increasing practical knowledge through learning from the experience of others;
- Developing working solutions to cultural, linguistic, or operational problems;
- Making existing synergies in areas of law enforcement cooperation, integrated border management, and the criminal justice systems more effective; and
- Cultivating trust and capacity-building beyond sport to enhance collaboration in other sectors or areas of common interest.

## 2. Cooperation through the Planning Process

In order to prepare and deliver a successful MSE, cooperation with international and other key stakeholders must begin in the very early planning stages and continue through to the post-event stage.

### *Exploratory Phase*

A country that is contemplating hosting an MSE must not only consider its own capacity to host a successful event, but also the available capacity and the level of commitment of potential partners. Early security-related deliberations ought to examine potential risks and the wider threat environment, including any existing or emerging geopolitical tensions of neighbouring and/or participating countries that may impact the event. Security authorities also ought to conduct preliminary assessments of security factors and make an inventory of their own available resources, financial and otherwise, as well as those of potential contributing stakeholders. Early consultations with key stakeholders are essential to establishing effective working relationships throughout the planning and delivery of an MSE (See Chapter V on Considerations Before and During the Bidding Process).

### *Bidding Phase*

In the bidding phase, it is recommended that international stakeholders who will be able to provide prospective bidders with a comprehensive picture of ‘on-the-ground’ security challenges, requirements, expectations, and opportunities be engaged. Building on preliminary consultations conducted during the exploratory phase, this may involve:

- Observer missions jointly undertaken by bidding committees and representatives from national security authorities to other MSEs to get a clear overview and gain insights on security considerations in terms both of opportunities and challenges.
- Transnational assessment of threats or geopolitical factors, capacity inventory available internationally (i.e., what resources and support are available); or
- Sharing of best practices and lessons learned experiences from other Host Authorities.

### *Planning Phase*

In this phase, planners should set out the groundwork for collaborative efforts, including setting the mission objectives, strategies, and operations plans. This phase requires extensive coordination between stakeholders to develop the legal and structural frameworks for collaboration (see Chapter VI on Legal and Institutional Frameworks), assess and mitigate the risk environment, and take stock of available resources and coordinate these (see Chapter VII on Planning Tools in the Security Planning).

### *Implementation Phase*

Ongoing collaboration and communication between stakeholders, particularly between law enforcement agencies and on-the-ground security personnel, during the event will address issues such as monitoring and assessing real-time threats, border control, and coordination of security resources.

### *Post-event Phase*

Post-event evaluation of security operations is critical for measuring performance, identifying best practices and gaps (see Section 3 on Post-Event Evaluation and Knowledge Transfer, in Chapter VII on Security Planning). In this phase, partners have the opportunity to assess the efficacy of their relationships where they can build on their strengths and where they can design improvements to support future collaborations. This phase also presents an important opportunity to produce legacy materials - tools, best practices, and recommendations - that can be shared with other prospective host authorities.

## 3. Foundations for Effective Stakeholder Cooperation

For countries that are directly involved in an event, either as participants, by proximity or in other roles, collaboration for MSE security planning is an opportunity to develop valuable relationships around knowledge and information exchange. This can improve and enhance the ability of each partner country to monitor and respond to threats within its borders.

For civil society or private-sector stakeholders, it is an opportunity to advance agendas on important social issues or to expand business prospects. Cooperation between public policing agencies and private security agencies may lead to greater collaboration in day-to-day policing operations (e.g. whereby private security providers take over tasks that require less training or specialisation). Ensuring there is a common understanding as to how security objectives can be achieved and how approaches are put into practice – something that is essential to effective collaboration.

Enhanced cooperation between stakeholders should be based on shared values. Mutual understanding and commitment to ethical standards and good governance, political neutrality and non-discrimination are all essential to ensuring partners are able to achieve security-related objectives.

# 4. Types of Stakeholder Cooperation

There are three main types of stakeholder cooperation which will be explained in this section: Inter-agency cooperation, international cooperation, and multisectoral cooperation and Private-Public Partnerships (PPP).

## 4.1 Inter-Agency Cooperation

Inter-agency cooperation is a critical component of secure MSEs.[71] This type of cooperation will be used in several aspects of event security, including monitoring and surveillance, on-site policing and security, public health, and emergency response. It will often require the coordination of local, national, regional and international partners. While these partners can significantly enhance knowledge as well as expertise and resources, communication and logistical coordination are complex and can be further complicated by differing objectives, conflicting interests, or even rivalries between agencies. This is particularly true in the context of those MSEs which are short in duration, as these usually provide less time to establish the systems and infrastructure needed to create solid and cohesive collaboration mechanisms. The challenge with a hierarchical organization is to determine the optimal configuration of the managing partners and the mechanisms that will coordinate mandates and resources to support the event.

It is also important to nurture relationships in order to lower and ultimately break down inter-agency barriers. This may be achieved by formal means, such as appointing liaisons who can inform and clarify the roles, responsibilities, and expectations of each agency and the organizing authority. Informal linkages between agencies, such as interaction with acquaintances or former colleagues, should also be encouraged to enhance inter-agency collaboration.

Furthermore, printed as well as online documentation, including guidebooks and written agreements, are very useful in enhancing inter-agency collaboration.

[71] Bistaraki, Angeliki and McKeown, Eamonn and Kyratsis, Yiannis. (2018). “Leading interagency planning and collaboration in mass gatherings: public health and safety in the 2012 London Olympics”. *Public Health*, 166, 19-24.

These networks are designed to:

- establish or strengthen ties between local, national, and international security agencies as well as private-sector entities that are involved in MSE security; and
- facilitate the gathering, analysis, and sharing of intelligence and security data between the various stakeholders, including law enforcement and private firms employed at the event.[72]

## 4.2 International Cooperation

While security-related concerns cover a broad field involving many stakeholders, the main aspects to take into consideration can be classified into bilateral and multilateral agreements, threat risk assessments, information sharing, resource sharing, capacity building and technical assistance, spotters and security networks.

### a) Bilateral and Multilateral Agreements

Bilateral and/or multilateral agreements between international partners support international cooperation during an MSE on topics such as border control or the sharing of intelligence or resources (e.g., law enforcement personnel, technology, or best practices); such agreements set out countries' commitments as well as associated financial obligations. In some instances, addendums may be placed on existing bilateral agreements.

While multilateral forms of cooperation are often viewed as more effective and a standard means to coordinate mutual assistance among countries, bilateral solutions can be designed to fit the needs of individual countries better, put more robust collaboration measures in place, or develop longer-term, and more complex, security frameworks.

### b) Threat / Risk Assessments

Identifying the unique threat profile of an MSE, and how to prevent or respond to those threats, requires a high degree of national coordination, as well as input from a range of international stakeholders, including international policing agencies, sports federations, and specialized security delegations. Threat assessment and evaluation is a continuous process throughout the planning and implementation phases of an MSE.

[72] Ludvigsen, J.A.L., (2020). "The more, the merrier? Euro 2020, transnational collaboration, opportunities and challenges". (DOI: 10.1080/14927713.2020.1745673) .

### c) Information Sharing and Intelligence Exchange

Information-sharing and intelligence exchange of real-time data on criminal activity are mechanisms that feed ongoing monitoring activities to identify and assess threats for the duration of the event. Information-sharing aims to provide the necessary information to neutralize potential security threats or counter criminal activities in advance of, or during, an MSE.

Exchanging sensitive information that is directly related to national security is particularly challenging and can be further obstructed by differences in legislation, operational methods, procedures, the geopolitical landscape, or a lack of bilateral or multilateral treaties. There may be instances where some Governments consider that sharing certain information will negatively impact their national interests or image. There may also be reluctance on the part of some international organizations to share the personal data of participating personnel for advance security checks and threat assessments. In such cases, international police organizations, such as INTERPOL and regional police organizations, e.g., ASEANAPOL, AFRIPOL, EUROPOL, AMERIPOL, GCCPOL and AIMC, amongst others, can support, facilitate, and enhance cooperation between national law-enforcement agencies.

Information-sharing mechanisms for MSE security are often built upon existing relationships with other countries; in their absence, these mechanisms should be built within existing infrastructures for international intelligence exchange. For example, for each Olympic Games event since Atlanta 1996, organizers have created an Olympic Intelligence Centre (OIC) to assemble information and risk assessments based on cooperation and information-sharing protocols involving over a hundred countries and international organizations. The support of international policing agencies is critical with respect to intelligence gathering and sharing.

### d) Resource Sharing

The secondment of police officers to support the host country’s forces provides not only a greater law enforcement presence and capacity but also resonates with fans when "their own" police are present at an event. These types of secondments may also extend to emergency response, health, and other security-related sectors, depending on the nature of identified threats around a specific event. Host Authorities may also benefit from borrowed equipment or technology-based platforms from international partners. However, not every stakeholder will have equal levels of capacity or resources to contribute. A capacity assessment, with input and analysis provided by multi-disciplinary subject matter experts, is recommended to determine the capabilities of each partner and to provide a road map for building the necessary security capacity (see Chapter VII on The Security Planning).

### e) Spotters

As part of international cooperation agreements, international partners may provide experienced, accredited spotters who are familiar with participating team supporter communities and can improve police and security personnel's understanding of expectations and potential issues that may be disruptive to the MSE.

During an MSE, designated spotters[73] support policing operations by gathering live and relevant information and intelligence on supporters and ensuring appropriate deployment of policing or security resources. They may also serve as community officers, particularly at football events, acting as links between the police and clubs' supporter communities. Spotters can help increasing trust and confidence between the authorities and supporter communities. Furthermore, as uniformed and highly identifiable individuals in a crowded environment, spotters act as a visible crime prevention tool, influencing crowd behaviour.

### f) Capacity building and technical assistance

International and regional organizations can offer extensive assistance to Host Authorities in planning and executing security measures, including by providing technical support and contributing to capacity building. Like other international stakeholders, they should be engaged early in the planning process and can play a crucial supporting role in a variety of areas. The organizations listed below play a key role in ensuring security planners have access to the information, resources, and perspectives needed to create comprehensive and effective operations plans.

| | |
|---|---|
| **UNICRI's International Permanent Observatory (IPO) on Security During Major Events[74]:** Collects | **INTERPOL's Project Stadia[75]:** is working to develop international standards through training |

[73] College of Policing. (n.d.). *Policing football*. See https://www.app.college.police.uk/app-content/public-order/policing-football/#football-spotter .
[74] See http://www.unicri.it/index.php/ .
[75] See https://www.interpol.int/en/How-we-work/Project-Stadia .

| | |
|---|---|
| knowledge and expertise from past major events, absorbs and incorporates lessons learned, and delivers them in user-friendly formats and tools to requesting national authorities. The IPO also offers major event security planners, upon request, a range of mentoring and quality-assurance services that draws upon a global bank of experts, all of whom have held key security positions at past major events. | programmes and expert group meetings and is capturing good practices and lessons learned before, during and after major international sporting events. Project Stadia's Knowledge Management System (SKMS) also provides real-time information on emerging incidents, events and emergencies and includes:<br>• a comprehensive knowledge repository of good practices in all aspects of major sporting event security, which all member countries can contribute to and benefit from; and<br>• an online collaborative platform where experts in the field can share, discuss, analyse and publish information on the evolving aspects of major sporting event security. |
| **The European Union Agency for Criminal Justice Cooperation (Eurojust)**[76]: Provides support in a variety of sport-related security issues, including the prevention, investigation, and prosecution of crimes committed by football hooligans at MSEs, doping and the trade of illegal doping substances, and digital crime. | **The European Union Agency for Law Enforcement Training (CEPOL)**[77]**:** Delivers a course on Public Order - Crowd Management and Security During Major Events PPP (House-EUSEC) which aims to deepen the knowledge and increase the competences on the level of security required for large-scale events and of cross-border cooperation in that context. It also aimed to improve threat assessment and management of major public events in order to prevent/effectively contain attacks carried out by lone-actor terrorists or violent lone criminals. |
| **The Organization for Security and Co-operation in Europe (OSCE)**[78]**:** This Vienna-based international organization with 57 members states has a comprehensive approach to security that encompasses politico-military, economic, environmental and human-dimension aspects. Its counter-terrorism efforts cover a broad range of | **The World Health Organization (WHO)** [79]**:** Mass gatherings at sporting events attract millions of international and national host country travellers, who may put themselves at risk of acquiring local endemic infectious diseases. During the 2013-2016 Ebola virus disease (EVD) outbreak in West Africa, three major sports events were held in the region with |

[76] See http://www.eurojust.europa.eu/pages/home.aspx .

[77] See https://www.cepol.europa.eu/education-training/what-we-teach/residential-activities/432017-public-order-security-during-major .

[78] OSCE Regional Workshop, see www.osce.org .

[79] See https://www.who.int/publications/i/item/key-planning-recommendations-for-mass-gatherings-in-the-context-of-the-current-covid-19-outbreak .

| | |
|---|---|
| activities, e.g. in the form of workshops such as the regional workshop on the Protection of Critical Infrastructure Against Terrorist Attacks in the OSCE area. | participation from a broad range of African countries. WHO missions were conducted to the host authorities to provide rapid technical support[80] in strengthening public health capacities and to advise on specific prevention and response strategies. Other transnational arrangements, such as screening travellers at airports and accessing specialised laboratory testing facilities, were also put in place to support public health security.<br>WHO has brought together rapidly all main international and continental sports bodies and specialized agencies to promote a common approach during and in the aftermath of the coronavirus pandemic. Sports bodies and relevant stakeholders have produced a set of key planning recommendations for mass gatherings in the context of COVID-19 related threats. |
| **International Atomic Energy Agency (IAEA)**[81]**:** The IAEA is the world's central intergovernmental forum for scientific and technical cooperation in the nuclear field. As part of security planning for public events, including large-scale sporting events, IAEA provides detection equipment, staff training, and information to address nuclear security threats, which have the potential for severe health, social, psychological, economic, political and environmental consequences.<br>IAEA developed an Implementing Guide on Nuclear Security Systems and Measures for Major Public Events. It represents a sound basis, drawn from experience, for raising awareness about nuclear security systems and the measures to be applied for such events. | **NATO's Defence and Related Security Capacity Building Initiative (DCB):**[82] Supports project stability by helping partners improve their defence and related security capacities, as well as their resilience. DCB can include various types of support, ranging from strategic advice on defence and security sector reform and institution-building to the development of local forces through education and training or advice and assistance in specialised areas such as logistics or cyber defence. |
| **Council of Europe:** The Standing Committee of the Council or Europe Convention on Spectator Violence (ETS No. 120), as well as the Committee on Safety and Security at Sports Events of the Saint Denis | |

[80] See https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance .

[81] See https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1546_web.pdf .

[82] NATO. *North Atlantic Treaty Organisation*, see https://www.nato.int/ .

| | |
|---|---|
| Convention (CETS No. 218), carry out monitoring activities namely to countries organising MSEs and provide technical assistance in partnership with national and cross-European public and private stakeholders. | |

Smaller regional organizations may also have designated security officials. In many cases, sports organizations interact with national and international stakeholders through a dedicated liaison officer who participates in planning meetings, shares pertinent information and recommendations, and serves as a connecting link between security planners and the organization.

## 4.3 Multisectoral Cooperation and Public-Private Partnerships

MSE security planners have the opportunity to draw on an extensive pool of cross-sectoral organizations to support security planning and operations. Each of these stakeholders from the world of sport, the business sector and civil society can provide unique assistance, grounded on special knowledge, access to information, experience and resources, to enhance security efforts.

### a) Local Organizing Committee (LOC) and International Sports Federation (ISF)

Joint planning and an extensive consultation process between the LOC, the ISF and hosting authorities tasked to secure an MSE must be fine-tuned, based on the specific context, regulations, and legal codes of the Host Authority.

International best practice, lessons learned from previous MSEs and guidelines should inform the joint coordination process between the LOC and the Host Authority’s law-enforcement agencies. This cooperation is formalized through a series of agreements between the Host Authority, the ISF and the LOC tasked with organizing the MSE at the local level.

Once the right to host an MSE is granted, the LOC, which can take different legal forms, public, private or mixed, is generally established. Thereafter, the drafting of binding agreements between the ISF and the local sports federation (e.g., Organizing Association Agreement between FIFA and the South African Football Association for the 2020 FIFA Club World Cup™) and between the host city and the LOC starts. This is one of the provisions stated in the binding agreements signed between the ISF and the local sports federation. The LOC is usually fully dependent and controlled by the host country association, which is ultimately responsible for the entire organization, staging and hosting of the event.

- **Roles and Responsibilities**

Even though the role of the LOC security section evolves during the life cycle of the project, its primary responsibility consists of coordinating and executing all MSE security measures at the level of the venues. Detailed operational plans are drafted for all official venues managed by the LOC, including event venues and parallel events (e.g. Olympic Park, FIFA Fan Fest) that take place during the competition. These plans require review and approval by government law-enforcement agencies, which are ultimately responsible for the safety and security of the MSE.

- **Intra and Inter-Cooperation**

LOCs are large, complex organizations consisting of separate Functional Areas (FAs) delivering capabilities such as Sport, Logistics, Transport and Protocol. Intra-coordination is required between LOC Security and other FAs to ensure security requirements are incorporated within the operations of other FAs. For example, venue client service-level agreements, drafted by the FAs (e.g. LOC Protocol, Transport, Sport) during the planning phase, inform venue design, overlay and access points impacting the venue security layout.

In each aspect related to the implementation of MSE security measures, training and readiness capabilities, law-enforcement agencies oversee the decision-making process as many of the measures developed for the MSE will be retained as a legacy to assist in maintaining effective and efficient policing in the Host country after the competition.

LOC inter-cooperation is also needed between various FAs and external government public-safety agencies, as a number of FAs have security dependencies to conduct their activities.

Furthermore, the geographical demarcation of responsibilities between the LOC and law-enforcement agencies in terms of security for the event requires an integrated plan.

- **Relations between the LOC and ISF**

The role of international sports federations in the security of an MSE varies, depending on the nature of the event and the threat environment. In most cases, the ISF will serve as an important resource for security planners due to their special knowledge (e.g., insight into the behaviour of fans and supporters), their familiarity with best practices, their experiences when it comes to lessons learned, or for regulatory guidance based on their role in previous MSEs. They will also often play a central role in communicating security measures and procedures to athletes and coaching staff, providing any required training and establishing reporting mechanisms for athletes and staff to signal suspicious situations or potential criminal activity.

Furthermore, ISF can offer additional value (e.g., through the provision of various resources, training, and awareness programs) for local stakeholders, including stadium/venue operators, private security agencies, or any organization involved in the MSE supply chain.

As per requirements stated in the agreements, such as the Organizing Association Agreement (OAA), the host national sports association is ultimately responsible for the entire organization, staging and hosting of the competition. Therefore, the LOC is established to fulfil this function. However, the host national sports association ought to retain the ability to fully direct and control all decision-making and activities of the LOC with respect to the organization and staging of the MSE, based on the rules and regulations issued by the ISF as the rights-holder of the competition.

### b) Relations with the Business Sector

PPPs are an increasingly popular instrument for enhancing security and safeguarding MSEs. One of the most valued benefits of such partnerships is resource sharing, including real-time intelligence gathering and analysis, social-media monitoring, threat and behavioural analysis, situational awareness, active-shooter/assailant training, workplace violence prevention and awareness, improvised explosive device (IED) explosives training, lessons learned and best practices.

In most cases, business-sector partners are also an essential source of funding to boost limited government resources. They bring greater efficiency and flexibility to many aspects of MSE operations and improve the overall quality of the event. They are also a “force multiplier”, reducing the workload of police and national security agencies and shorten the response times during a security event. They often have specialized knowledge that can be invaluable for various aspects of security planning and threat/risk assessment - particularly in technology and cybersecurity - that extend beyond the immediate event venue.

However, expanding the network on security-related matters to private sector stakeholders does carry potential risks and challenges. The most significant risk is the possible misuse of sensitive information.

On the Government's side, law enforcement may not be comfortable with, or may not even be legally permitted, to share security-related information, while business sector companies may be reluctant to let privileged business information enter the public record. It is recommended that personnel directly involved in security planning and implementation be vetted and that formal information-sharing agreements be put in place with private-sector partners.

- Owners/Managers of Vulnerable Targets

Although Governments bear the primary responsibility for protecting facilities, including against terrorist attacks, the private owners and/or operators of such sites must also take steps to address the related security needs and reduce their vulnerabilities. Governments, community leaders, and private-sector actors must cooperate to identify ways to mitigate the related risks and threats and, ultimately, to prevent such attacks from occurring. During MSEs, these partnerships may be formed to protect not only event-related venues, but also soft targets[83] in the surrounding community. Effective protection of such targets requires not only the implementation of physical protection measures but also the development of strong and resilient communities and close engagement with civil society and local leadership.

As with all areas of cooperation, information exchange between public authorities and critical infrastructure operators is vital. Best practice in these exchanges indicate a two-way information flow between partners that address:

- *Threats:* Law enforcement and intelligence services should convey threat information so operators can conduct necessary risk assessments and put mitigative measures in

[83] See UNICRI's PPP Handbook. Soft targets include parks, markets, shopping centres, train and bus stations, hotels and resorts, cultural, historical, religious and educational centres, multinational company premises and financial centres, cruise liners and touring coaches.

place. Operators must communicate these results back to the authorities to ensure better modulation of mitigation plans.

- *Suspicious activities:* Critical infrastructure operators should report unusual situations that may not be sufficient to trigger an alarm but may reveal an impending threat when examined in the context of similar events or corroborating sources.
- *Incident data:* Lessons learned from past incidents, including actions taken, may offer important insights into prevention, risk management, and recovery from similar situations during an event.[84]

### Official Sponsors and Corporations

Sponsors and large corporations play a major role with regard to the financial sustainability of MSEs. These relationships not only bring bottom-line returns on investment but also provide opportunities to align business with the positive values inherent in sport.[85] Given the direct link to their brand and also large numbers of their staff deployed during the event, official sponsors of MSEs have a fundamental interest in the event's security.

The nature of cooperation between MSE organizers, security authorities, and sponsors is two-fold: on the one hand, planners must consider security measures to protect sponsor assets and, on the other, establish how sponsors can contribute to security planning and operations.

Security planning must incorporate elements to protect sponsors and corporate companies who may become targets of criminal or terrorist attacks. In these cases, collaboration between the event and organizational security teams will be useful in assessing the threat environment and identifying the capacity and resources at hand to mitigate identified threats.

At the same time, most corporate and sponsor organizations will employ experienced, retired law-enforcement professionals who have worked in previous events and can offer opinions and ideas on best practices. Regular security briefings between sponsors, security organizers, and

[84] United Nations. (2018). *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*. Counter-Terrorism Committee Executive Directorate and Office of Counter-Terrorism, page 96. See https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

[85] Fuller, J. (2016). Promoting integrity in sport: A sponsor's perspective. In *Global Corruption Report: Sport*. Transparency International. See https://www.transparency.org/files/content/feature/6.5_PromotingIntegritySponsors_Fuller_GCRSport.pdf

law-enforcement authorities can offer a useful platform for information exchange and will also provide reassurance to sponsors.

Cooperation between sponsors and other corporate stakeholders can be optimized in a variety of ways. It is recommended to involve them early in the planning dialogue as this may reveal new perspectives, information, or approaches that can be employed as part of the wider security plan. For example, the security cultures, procedures, and risk assessment/mitigation models applied by global corporations might provide important insights for security planners. Including sponsors and corporations in early capacity assessments can also prove valuable for enhancing and coordinating security resources. Establishing public-private associations could also promote knowledge-sharing and best practices, based on prior or specialized experience.

- Big Data

One of the major challenges, and at the same time opportunities, available to authorities of host countries is the availability and use of big data gathered at the international level. The capacity to collect, analyse, and use large amounts of data is likely to become a key element of the security preparations of an MSE.

As IBM (U.K.) describes it:

> Big data has one or more of the following characteristics: high volume, high velocity or high variety. Artificial intelligence (AI), mobile, social and the Internet of Things (IoT) are driving data complexity through new forms and sources of data. For example, big data comes from sensors, devices, video/audio, networks, log files, transactional applications, web, and social media — much of it generated in real-time and on a very large scale.
>
> Analysis of big data allows analysts, researchers and business users to make better and faster decisions using data that was previously inaccessible or unusable. Businesses can use advanced analytics techniques such as text analytics, machine learning, predictive analytics, data mining, statistics and natural language processing to gain new insights from previously untapped data sources independently or together with existing enterprise data.[86]

[86] See https://www.ibm.com/uk-en/analytics/hadoop/big-data-analytics .

In an MSE context, such capacity will relate to everything from ticket purchasing to crime spot prediction models and terrorist profiling. New data-handling technologies are integral to the planning of MSEs but, if not used appropriately or if the data upon which the technology relies contains inherent bias, come with their own set of human rights concerns and security-related issues,-- including cyberattacks, privacy and breaches of the right to privacy, equality and non-discrimination.

For example, collecting data on access (e.g., time and number of people) to stadiums at turnstiles can help security personnel track people flows and improve security deployments or model flows for crowd management and contingency planning. Biometrics and data analytics are also key areas of innovation that enable international law-enforcement agencies, such as INTERPOL and Europol, or border control agencies, such as the European Border and Coast Guard Agency (Frontex) to address today's security challenges. Biometrics, including facial recognition technology, can be an important tool for identifying criminals from video surveillance footage. Analysis of data intelligence is also key to identifying crime patterns, establishing links between perpetrators and investigations, and identifying threats.

However, there are challenges that must be considered.[87] As mentioned in Chapter V on Legal and Institutional Frameworks, MSE organizers and stakeholders must navigate the complexities of data privacy laws (including data collection and data protection laws) as well as ethical norms. As these vary from country to country, it creates an uneven terrain in terms of the type of data authorities may access or share.

From the planning perspective, organizers should leverage the knowledge, experience, and expertise of private sector partners to develop and incorporate appropriate measures to prevent or respond to cyberthreats. (See Chapter II on The Guide; box on Cyberattacks)

- Service Providers

Every MSE will need to engage private-sector service providers in numerous areas, including construction, venue setup, catering, cleaning, and transport to satisfy the needs of athletes, officials, spectators, and media. These entities may also be supplemented with a large army of volunteers. From a security perspective, organizers need to establish security protocols for each

[87] See https://journalofbigdata.springeropen.com/track/pdf/10.1186/s40537-019-0206-3 .

of these areas. Protocols should include communication strategies, training, vetting staff, and providing site-access authorizations.

There are a number of external service providers who should be involved in the security planning process. Sanitation, transport (e.g., airlines, rail, bus, metro), food and beverage, water and power utilities, emergency and health-care, and others certified providers should be engaged collectively in the early planning stages to achieve buy-in and establish standards.

- Private Security

Private security companies have a particularly important role in security planning. The public-private sector relationship can be challenging where public agencies are sometimes very uncomfortable with the private sector due to concerns around ethical and professional standards and quality of service. This may be mitigated to some degree by ensuring that private security companies that are involved meet recognized standards, such as ISO 18788:2015 (Management System for Private Security Company Operations by the Geneva-based International Organization for Standardization),[88] which provides a framework for the Security Operations Management System and outlines professional conduct, accountability to applicable law, and respect for human rights requirements. Public agencies do recognize, however, the limits of their capacity to supply all that is needed for organizing a major sporting event and acknowledge the need to work with the private sector in order to meet the expected level of safety and security.

In developing operations security plans, the roles and division of tasks between private security and law enforcement must be clearly delineated, and constant information exchange between these stakeholders is a must.

### c) Relations with Civil Society Organizations

Civil society, through local communities, non-governmental organizations (NGOs), supporter organisations, and individual spectators (especially those who are social-media influencers), play an important role in security planning for MSEs. Members from these groups are not only a source of local intelligence but can also provide important perspectives and insights on key issues such as human rights or local community impacts. Engaging civil society representatives

[88] See https://www.iso.org/standard/63380.html .

early in the planning process can establish important relationships for cooperation to ensure a successful event.

- **Local Communities.** Establishing mechanisms for connecting, consulting and collaborating with local community groups can help improve specific aspects of security planning and operations. For example, NGOs dedicated to special issues such as the prevention of youth radicalization and violent extremism can enhance understanding of the local context and provide expertise and tools which might be useful for security planning. In the safety field, local communities are also a source of information, e.g. regarding people with special needs, such as disabled persons who should receive extra consideration in crowd management or at security checkpoints.
- **Supporter Organizations.** Early interaction with supporter organizations can inform best practices and thereby minimize conflict between fan groups or backlash against security personnel. They can also offer an opportunity to establish a positive narrative to promote among fans, or to facilitate cooperation between supporters' organizations directly or through larger networks like the Football Supporters of Europe -- to share ideas and build crucial relationships in support of peaceful games.

All successful collaborations, including those that cross the public-private-civil divides, have common themes

- ✓ Inclusion of key stakeholders
- ✓ A clear mission statement and a detailed assignment of responsibilities
- ✓ A common governing document or framework for collaboration
- ✓ Strong leadership from both the public and private sectors
- ✓ Goodwill, trust, and respect between participants
- ✓ Transparency and accountability in interactions
- ✓ Building situational awareness through intelligence sharing
- ✓ Regular and effective communications
- ✓ Round-table discussions on topics related to crisis management
- ✓ Post-event "after-action" review and analysis

Source: IACP. (2004). *Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder*; see https://www.theiacp.org/sites/default/files/2018-08/ACFAB5D.pdf

**Recommendations:**

**Stakeholder Cooperation**

### General principles

→ Understand “stakeholder collaboration”, based on shared values, as a prerequisite for MSEs to bring about a secure environment. Ensure that close and effective levels of stakeholder collaboration are established in the very early planning stages and are maintained right into the post-event phase.

→ Engage and encourage a wide range of stakeholders to share their particular security-related concerns (e.g. national police, fire department, Red Cross, health authorities, participating sports organizations, and authorities responsible for sports venues, logistics, civilian protection, volunteers, VIPs private and public security, transportation (air and road), cyber and information technology).

→ Conduct a capacity assessment, with input and analysis provided by multi-disciplinary subject matter experts, to determine the capabilities of each partner and to provide a road map for building the required overall security capacity.

→ Provide vetting systems for individuals directly involved in security planning and implementation.

→ Establish security protocols for construction, venue setup, catering, cleaning, volunteers, and transport areas. Such protocols may address communication strategies, training, staff-vetting requirements and site access authorisations.

### International cooperation and outreach

→ Ensure that threat assessment by national intelligence and security services are conducted in close and regular consultation with international partners, including countries from where a significant influx of fan groups is expected.

→ Consider the signing of specific bilateral and/or multilateral agreements with international partners as a tool to cement cooperation and support concrete actions in the run-up to and during the MSE.

→ Leverage the often-extensive assistance that international and regional organizations can offer to countries in planning and executing security measures before and during an MSE.

→ Involve all countries represented at the MSE in security preparations and in resource-sharing as a condition to enhance security capacities and reduce potential threats and risks.

### Information sharing

- → Support stakeholder collaboration by establishing effective information-sharing arrangements, including by a) setting up an information technology platform that is compliant with applicable regulations and that can be used to share data securely and seamlessly between stakeholders; b) setting up event-specific platforms for participating countries where relevant security information can be collected and analysed.
- → Use the secure channels offered by international and regional law enforcement organizations to exchange operational information with other countries.

**Engagement with the private sector**

- → Develop functional public-private partnerships (PPPs) to enhance security and to safeguard the public during MSEs.
- → Encourage stakeholders from the private sector to contribute to inclusive information exchange with a view to sharing risk assessments, adding value/efficiency/depth to the security dialogue as well as, where appropriate, developing security solutions. Public-private information sharing should be supported by the conclusion of specific agreements.
- → Throughout the security planning and implementation process, involve in the discussion owners and managers of  a) critical infrastructure that will deliver essential services to the MSE; and b) sites (e.g. soft targets) which may become targets of attacks in relation to the MSE.
- → Hold regular security briefings between sponsors, security organizers and law-enforcement authorities with a view to, among others: a) discussing potential security measures to protect sponsors who may become targets of criminal or terrorist attacks; b) exploring how sponsors can contribute to security planning and operations; and c) leveraging sponsors' marketing expertise to develop appropriate messaging around security measures.

**Engagement with civil society**

- → Recognize the crucial role that civil society (in the form of local communities, non-governmental organizations, supporter groups, and influential individual spectators) plays in the security planning of MSEs and determine in advance what civil society can contribute when dealing with the aftermath of security-related incidents.
- → Encourage stakeholders from civil society organizations to contribute to an inclusive information exchange with a view to sharing risk assessments, adding value/efficiency/depth to the security dialogue as well as, where appropriate, developing security solutions.
- → Work with NGOs, including local social-justice organizations, to a) share knowledge, build capacity and increase accountability around critical human rights issues; and b) obtain advice on

how issues such as racism, discrimination, poverty, or civil rights can be considered as part of security preparations and operations.

→ Develop interaction with supporters' organizations to inform best practices as a way to minimise conflict between fan groups or backlash against security personnel.

# VII. THE SECURITY PLANNING

Once an MSE is awarded, the security planning has to be initiated, leading to the creation of a comprehensive system, which can ensure an effective event security structure.

The security planning will have to capitalize on the vision developed at the time of the presentation of the Bid (see Chapter III on Foundations of Security at Major Sporting Events, Leadership and Vision) in order to ensure continuity across the overall process, review it in the light of possible new challenges and changes in the global, regional and local contexts, and define a clear roadmap leading up to the event.

The purpose of this chapter is to draw attention to the security-planning process by focusing on the primary partners, their mandates and how they can work together to maximize the use of resources and create other efficiencies as a means of controlling costs during the planning phase and operations.

It also focuses on the requirement to ensure proper management, taking into account the foundations and all elements that should drive the security planning, including leadership, good governance, public and private partnerships, intelligence, sound use of human and material resources, and effective communication.

Within an MSE context, the establishment of a Senior Executive Team (SET), composed by the most senior representatives of the Government agencies, organizing committees and the business sector is critical to the success of the event. The SET has the primary responsibility of ensuring that the broader mission of the MSE is focused and aligned. Similar supporting frameworks need to be created for the various functional areas of the organization of an MSE, including security. These other frameworks are to have a direct and interdependent relationship with the SET.

The planning system proposed below brings together multiple agencies with diverse backgrounds and engages them at various levels as executive leaders, senior leaders, mid-level managers and tactical planners.

- One Ministry acts as the Government’s lead security agency responsible for the event and is the Government representative on the SET.
- The Sports Ministry (in the absence of a specific Sports Ministry, it could be the Interior Ministry or another one) offers the required administrative, logistical and oversight

support for events within its domain. For MSEs such as Olympic Games or FIFA World Cup™ events, the Government will often create additional Cabinet-level infrastructures to enhance governance and service delivery.

- The Cabinet Committee is established and led by the Prime Minister/President or a designated Minister and is composed of senior Cabinet Ministers from Finance, Security, Public Works, etc. The Cabinet Committee oversees government policy, spending and legislation as it relates to the MSE.
- The Event Delivery Authority ensures a "whole of government" approach, involving several Ministries such as Finance, Interior (Home Office), Public Safety, Defence, Health, Transport, Justice, Immigration, Border Services, Infrastructure, and Foreign Affairs.
- The national and international Security and Intelligence community create a parallel but separate entity, sometimes known as the Security Committee with the responsibility for the safe and secure delivery of the event.
- The Government departments deliver their mandated services in support of the event and will coordinate their services with the Local Organizing Committee and the International Sports Federation (See Chapter VI on Stakeholder Cooperation, subsection 4.3 on multisectoral cooperation).

Now that the broader MSE interdependencies have been outlined, the linkages between the mission, leadership, and governance from a hierarchical perspective can be better understood.

As mentioned in the Introduction, every MSE should reflect a vision and sport-related values as a guide to meeting its desired end-state. This will also serve as a method of confronting "tricky" situations in an ethical way and forms the fundament for a multi-directional communication strategy.

It takes strong leadership at all levels to ensure that planning is mission-focused and in line with a collaborative governance model that involves all participant groups and organizations to ensure compliance with agreed-upon policies and procedures. For this reason, it will be essential to carefully choose the right leaders, that is, able and experienced personalities with strong interpersonal and communication skills who can harmoniously work together, based on a clear mandate.

# 1. The System

Security planning for an MSE is a massive and complex undertaking that requires proactive strategic thinking and engagement by senior Government officials, local organizers and business sector partners.

Planning cannot be based on an ad-hoc collection of ideas and thoughts but needs to be a well thought-out process to overcome a wide range of difficulties that may impact the planning process. The focusing of multiple partners is essential so that they are able to share the same values and can work together to accomplish a common mission, the identification of human and material resource requirements, and the provision of the means of building and putting in place a sustainable planning system - these are some of the challenges the lead security agency will have to tackle.

At its most basic, systems are comprised of three main components: inputs, processes, and outputs. This concept is demonstrated later in this Chapter.

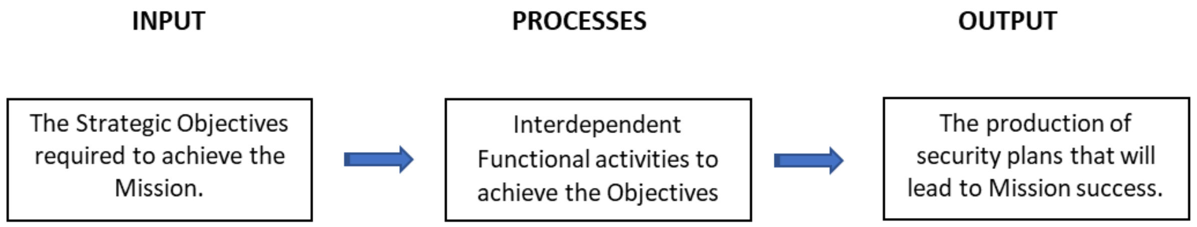

INPUT
PROCESSES
OUTPUT
The Strategic Objectives required to achieve the Mission.
Interdependent Functional activities to achieve the Objectives
The production of security plans that will lead to Mission success.

***Diagram 2 – This flow-chart demonstrates the primary system activities in terms of security planning.***

## 1.1 Characteristics of the Security Planning System

To construct a sufficiently coordinated system that takes inputs, processes them, and produces outputs to meet the organizational objectives, an understanding of the particular characteristics the system will need in order to be effective is required. In terms of system requirements to create security plans for a multi-agency organisation in a changing environment, the planning system:

- Should be capable of producing the type of plans required to meet the mission of the event. Are the system components efficient in terms of scope of work given the available time?

- Should, in terms of human and material resources, have the capacity to process large volumes of work within critical time windows.
- Should be able to overcome unexpected challenges that require a quickly formulated response. Venue changes, human-resourcing shortfalls, technology failures, responsibility disagreements, mobility issues, public health issues and weather conditions are just a few examples of contingencies that have to be met creatively.

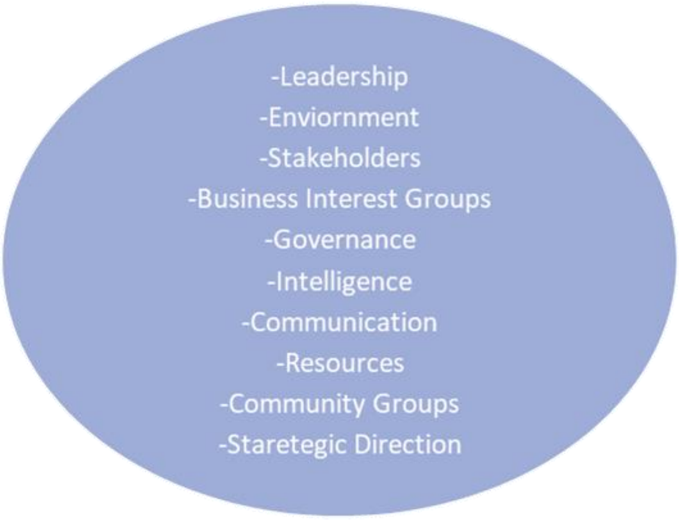


***Diagram 3: Characteristics and Elements of a Security Planning System***

## 1.2 Key Elements of the Security Planning System

A successful security-planning system needs to be built around a number of key elements; the main ones are listed below.

### *a. Leadership*

Experience has shown that two contrasting yet complementary and equally important leadership styles, i.e. relationship-oriented leadership and task-oriented leadership, are necessary parts of the leadership function. The relationship type of leadership requires a high degree of diplomacy to strengthen relations with strategic partners and to show concern for the needs of planners who are obliged to carry out the security-planning mandate. The task-oriented leader needs to motivate and emphasize task performance by setting goals, ensuring proper supervision, and making sure planning remains focused and on track. Both of these abilities are necessary for a multi-partner changing environment with competing pressures spread over a long period of time.

### *b. Good Governance*

Lessons learned from previous events demonstrate how critically important it is that a large and complex planning organization have a system of good governance to ensure its members follow the established process, policies, and operations sketched in the mandate. As explained in the introductory section of this Guide, the concept of Good Governance embodies, among other things, the values of respect for diversity and culture, the protection of human rights, gender equality, inclusiveness and a sustainable environmental approach.

### *c. Human and Material Resources*

Decision-makers must understand the complex undertakings of security planning and the requirement for input by experienced and skilled people from all stakeholders at each phase of the event: exploratory, bidding, planning and operational delivery phase.

To build a strong security system requires a considerable amount of research to ensure that the right capabilities and capacities are in place to respond to known needs and emerging challenges linked to the mission. To make the planning system work, assessments of the human and material resource requirements will be necessary.

The functional components of the security system will need to be defined with specific terms of reference to describe mandates, with clear roles and responsibilities, while also ensuring accountability.

Such elements are comprised of but not limited to advisory groups, senior managers, Joint Operational Planning Groups (JOPG), integrated risk-management groups, issues-management groups, and planning practitioners (See Diagram 3 above). At the same time, experience has shown that the placement of untrained and inexperienced planning personnel in these positions risks system breakdown, increased stress, lack of management confidence and failure to meet critical deadlines. For these reasons, and in line with the Saint-Denis Convention that requires that security personnel be appropriately equipped and trained (see Chapter VI on Legal and Institutional Frameworks), serious consideration should be given to the provision of training, focused on planning principles and requirements for a specific MSE to ensure an understanding of roles, responsibilities, and expectations for both public and private security personnel.

### *d. Security Design*

Security design or security engineering can be described as the design of the technical security systems utilized for MSEs. It is part of an overall integrated mitigation strategy which should be as user-friendly as possible and minimize the need for additional operational security, thereby ensuring that the overall level of security for an MSE is as effective as possible. Some elements of security are more efficiently undertaken by smart technology rather than by people. For example, the use of artificial intelligence (AI) technology to mine threat-related information that is in the public domain and available on social media has become an important aspect of MSE security.

The security design process should be initiated by the MSE organizing committee, ideally as early in the design process as possible. The risk owners (e.g. Government, local council, Ministry of the Interior, organizing committee) should be responsible for managing and reviewing the security design process throughout all the project design stages. Clear lines of communication should be established between the LOC security and key security stakeholders.

**Common Elements – Security Design**

| **Electronic Security Design** | **Physical Security Design** |
|---|---|
| • Video surveillance systems | • Fencing/barriers |
| • Access control systems (ACS) | • Blast / ballistic protection |
| • Intrusion detection systems (IDS) | • Hostile vehicle mitigation (HVM) |
| • Security management systems (SMS) | • Hardened areas |
| • Security network design and cabling | |

**Cybersecurity Design**

Cybersecurity design is included within the electronic security design process, e.g. secure network design, secure cabling, etc. Cybersecurity design should be included as part of the overall sporting event design process.

### *e. Technology*

From a technology perspective, information management systems are critical to the planning, implementation, and post-event phase of the event. The interface of computer and telecommunication networks significantly increases internal communications and information-management capabilities. The assessment of property space needs in terms of office space, furniture, transportation, and accommodation is an additional resource requirement.

Technology plays an omnipresent role in most people's daily lives, and it is no different when it comes to security solutions for an MSE. While the task of evaluating, selecting and finally implementing technology equipment and services can seem complex, it is possible to keep things simple by following some straightforward guidelines. In this section, we first define the relevant areas where technology plays a critical role and then share with the reader some best-practice approaches that can be applied to many MSEs.

When evaluating information technology (IT) solutions for MSEs, it is important to look across options and availabilities in three overlapping areas.

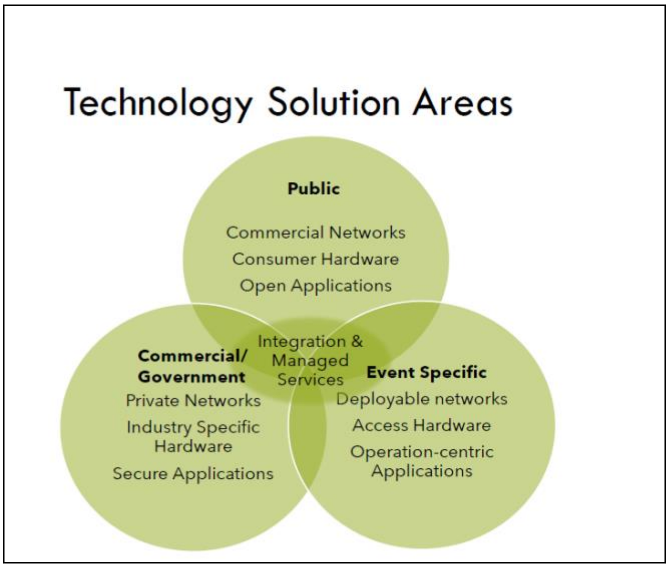


*Diagram 4: Technology Solutions Areas*

The first solution area covers the mainstream, commercially available networks, devices, and applications. These include IT vendors, service providers and value-added resellers (VARs) who are focused on delivering Business-to-Consumer solutions to the market. Secondly, there are  industry and Government-focused solutions that concentrate on specific operations such as transportation, public safety and utilities. Most well-established event and entertainment venues will have made at least some of their investment here. The third area covers solutions that are specific to event management, with a focus on ease of deployment, access and identity control, and command-centre operations. Each solution area complements the others, and with the right integration and planning, can be deployed alongside each other.

Decision-makers should focus on proven technologies that have been thoroughly tested and look for available user-approved solutions. If possible, planners should avoid trying new but untested solutions. In addition to being easier to budget and better to understand cost implications, established solutions will have event reference customers to speak with, and will have already dealt with customizing requirements to a local context.

Adopt open-source, legacy-compatible technologies, when feasible. Open-source software is software in which the source code used to create the program is freely available for the public to view, edit, and redistribute. Contrary to closed-source or proprietary software, an open-source licence encourages a shared community approach to the development, extension, and future compatibility of solutions.[89] Note that open-source MSEs solutions should only use open-source technologies that use established formats, specifications, and procedures. Furthermore, hybrid models that combine open-source and closed-source technology can be relevant, based on security and other needs.

### *f. Corporate Partners and Sponsors*

As explored to a greater extent in Chapter VI on Stakeholder Cooperation, key corporate partners and sponsors play a major role in the delivery and success of the MSE. This also extends to the event's security network. To the highest degree, Government security planners must be respectful of the agreements and expectations of the key partners and sponsors as these have made significant investments in terms of expertise, human and material resources, as well as finance. There are often mutually beneficial opportunities to collaborate on security matters as most of the key partners have their own security apparatus, which includes security practitioners and intelligence professionals – often former Government officials. Corporate partners also have material assets that can be shared in support of mutual security objectives/goals. In cases where the corporate partners and sponsors have bona-fide security professionals on their staff, they should be integrated into the appropriate Joint Operational Planning Group (JOPG), as per Diagram 6 below.

### *g. Strategic Communication Channels*

It is important to have seamless communication with the appropriate audiences and in an appropriate way. Effective internal and external communication strategies are, therefore, an

[89] See https://www.esri.com/news/arcnews/spring11articles/open-source-technology-and-esri.html .

essential component of the planning system. At the top end of the spectrum, there should be a clear incident-response and crisis communications plan in the event of a major security incident, whilst day-to-day communication within security teams needs to be equally seamless.

### *h. Intelligence Collection and Exchange*

The role of intelligence collection has become increasingly important in the era of terrorist threats against large crowd gatherings as in major sporting events. When it comes to securing any MSE, intelligence and timely information sharing through well-established channels involving both international and national intelligence communities as well as the various levels of public and private stakeholders involved in securing the event is crucial (see Chapter VI on Stakeholder Cooperation, the section on Information Sharing and Intelligence Exchange). Many countries have bilateral or multilateral information sharing arrangements in place, and these arrangements must be activated early in the planning of the MSE.

Intelligence is critical to the understanding of threats and the evaluation of risk. The intelligence information will determine the prioritization of resources and also determine the relative intensity of security operations across the entire event spectrum. Although the official Government intelligence networks are the foundation of the information collection and distribution, the value and depth of the private-sector and corporate intelligence capabilities should not be underestimated and should therefore be sought after.

The lead security agency, along with critical infrastructure stakeholders, must conduct *threat and risk assessments* of event venues and important non-venue sites. Information should also be gathered from open-source, real-time data on suspect activities, or covert operations long before the event takes place. Intelligence sources must produce timely and accurate reports throughout the event-planning phase to ensure plans and mitigation strategies evolve to meet security threats to the MSE. A good example of this was the London 2012 Olympic Games, where the U.K. Government set up a specific methodology to identify the types and relative levels of risk which could have hindered the effective delivery of a safe and secure MSE, thereby informing strategic-level decision making and planning.[90]

[90] See Olympic Safety and Security Strategic Risk Assessment (OSSSRA), UK Home Office, 2011.

With many MSEs taking place over multiple days and locations, there are significant security and public safety challenges in terms of mobilizing adequate resources and capabilities against a plethora of possible threats. There is a delicate balance that security planners need to ensure between the "accessibility for all" concept and the need to reduce perceived risks as much as possible.

## 1.3 Integrated Security Planning Strategy

Integration must be part of the overall strategy when planning MSEs. The challenge is to have several entities simultaneously work toward a shared mission while at the same time respecting their own mandates, policies, and directives.

For this reason, the lead security agency must implement strategies within the planning system to ensure inter-agency collaboration and to avoid organisational conflict and planning gaps. For instance, different agencies might have oversight for critical infrastructures (transportations systems, electric power, freshwater, waterways, etc.) that have a direct impact on venue operations. What would be the impact if a sporting stadium were to suddenly lose electric power or if primary transportation systems were to come to a halt during the Games' operations?

There is a requirement for critical infrastructure protection. However, the planning requirement is broader than this as it encompasses agencies responsible for border protection, air operations, marine operations, and land operations.

| Integration and Interoperability |
|---|
| An example of the critical aspect of integrated planning and interoperable capacity is the need to consider the unofficial sites/activities in the event security planning. This will have an impact on the contingency plans and the positioning of assets for rapid deployment in the event of an incident. Assets such as specialized equipment and personnel are limited, so they will often be available for shared duties. |

The "output" on an integrated planning system will be the production of joint, integrated, and standalone plans that are interoperable. Therefore, an integrated multi-organizational system must have a mechanism to ensure that plans are interoperable. This mechanism will be further addressed below under Section 2 on Planning Tools (the Deliverables).

Host Authorities will determine the design and implementation of the MSE security systems utilized for their specific event. No one security planning system is adaptable to all countries as each event is unique due to different opportunities, challenges, threats, and geopolitical circumstances. Government oversight, politically driven policies, financial constraints, and the ability to mobilize human and material resources within the required time frames have an impact on the planning and delivery of security. That is why systems must have the capacity to adapt to challenges.

Diagram 5 below represents a tried and proven integrated security planning system used to plan MSEs. This system contains all of the components referenced throughout this chapter.

Diagram 5 - The Security Planning System

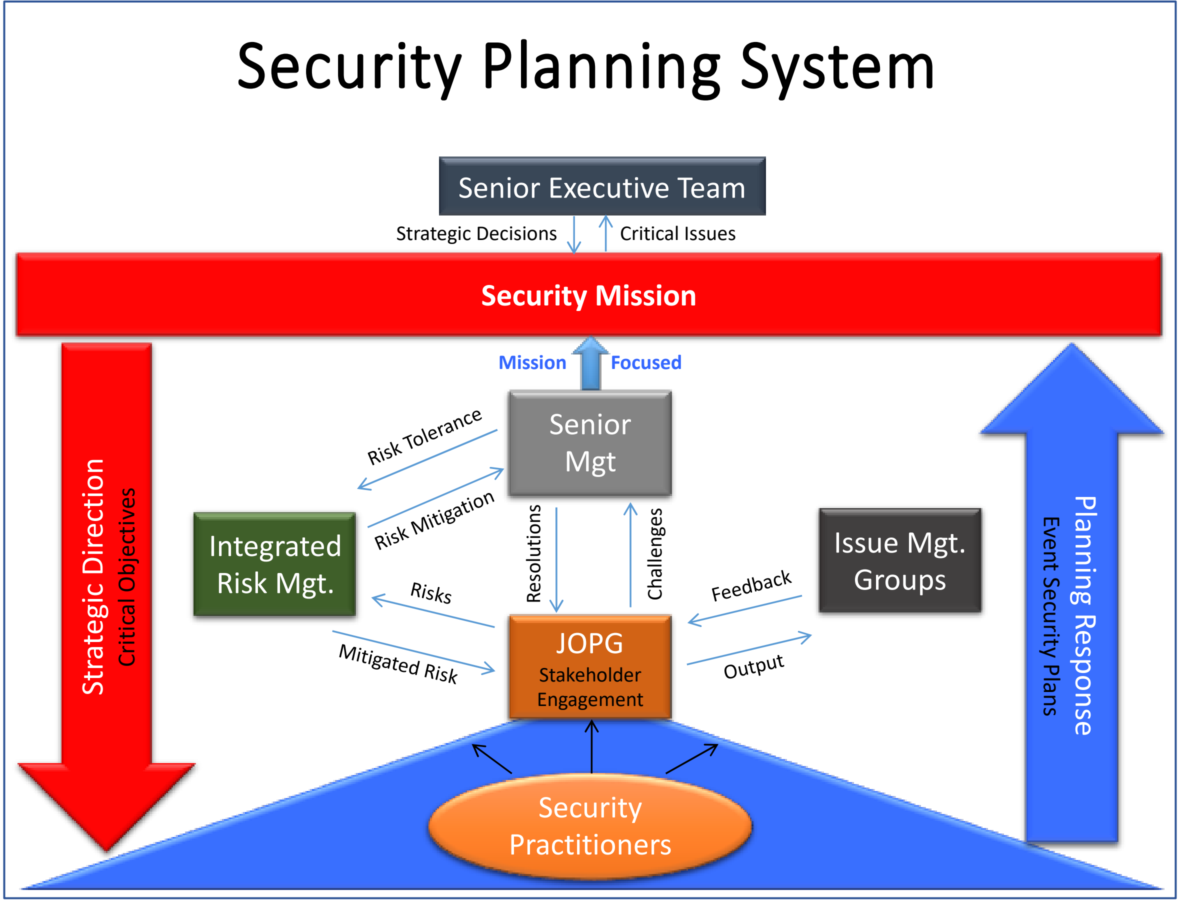


*Diagram 5: Security Planning System. Strategic inputs are represented in red, while the tactical operations responses are represented in blue. JOPG stands for Joint Operational Planning Group.*

## 2. Planning Tools (the Deliverables)

This section serves as a strategic guide to facilitate more detailed planning of the key security functions. It helps identify budgetary projections, planning gaps, and material and human resource needs. It also provides a framework for the identification and management of categories of plans and their evolution through the planning phase to a stage where they can be successfully executed.[91] And lastly, it establishes a *quality control process* that helps ensure

[91] The following is a conceptual approach to plan development and evolution based on operational considerations common to MSEs. It is not a methodology for a plan-specific development.

plans are interoperable and free of performance gaps well before they become part of the master security plan.

As mentioned, MSEs have become the targets of terrorists and other criminal actors; therefore, they require effective security plans. These include plans for securing venues, transportation systems, critical infrastructure, emergency operations, and cybersecurity defences among several other plans.

Of critical importance to the success of all MSEs is that planning start early and that it strike a balance between the hard security infrastructure and the soft atmosphere of the event. Security measures should be robust, effective and ever-present, but not appear threatening or overpowering. A clearly visible security presence is essential, but it should not instil a sense of fear or undue concern.

Before the plans and process for their development is explained in detail, it is important to reemphasize the difference between the interlinked concepts of safety and security as they generate a great deal of attention from Governments, host committees, and business-sector partners when it comes to MSEs. The safety and security terms are often used interchangeably but interpreted differently depending on what part of the world one is located. Planners must understand the difference between these closely connected concepts as they are foundational to the planning response.

- **Safety** can, in the MSE context, be understood as being free from danger or risk of injury or harm. Safety measures signal a "steady-state" which creates a feeling of confidence for athletes, spectators, and event staff. Safety planning must be focused on prevention and mitigation measures to manage accidental and unplanned negative occurrences.

| Safety Examples |
|---|
| ✓ The storage of hazardous materials such as gasoline for fuel generators could present a serious safety risk when stored close to athletes or spectators stands. |
| ✓ There need to be professional medical health care teams present, assisted by paramedics, ambulances, defibrillators, etc., strategically placed at various event locations. |
| ✓ Evacuation routes need to be clearly identified and visible to all staff, and there needs to be proper signage for the general public. |

- **Security,** in the context of an MSE, refers to the presence of measures which can offer protection and resilience against potential harm or damage caused by hostile forces who want to exploit vulnerabilities and bring about unwanted change. For instance, terrorist attacks present a high-security risk for soft targets. Security planning must focus on detection, prevention, and intervention for the protection of beneficiaries (athletes, spectators, staff) against malicious acts.

| Security Example |
|---|
| ✓ There must be a plan to detect and prevent acts of terrorism. Timely and accurate intelligence, covert operations, cybersecurity, and perimeter security all work to counter not only acts of terrorism but other intentional acts such as violent protests and destruction of property (See Chapter V on Legal and Institutional Frameworks). |

## 2.1 Categories of Plans

Like factories which can manufacture different products at a reasonably fast pace, planning systems can be seen as “factories” that manufacture executable blueprints. In terms of the manufacture or development of MSE security plans, there are two primary planning considerations.

First, plans must respond to the security needs of the event programme (such as programme scope, when and where what will take place, over what length of time, and the specific nature of individual programme activities). Second, it is essential to make threat assessments for the security of athletes, spectators, and staff present at the event. These two considerations must be the ongoing focus and concern as plans evolve from an early formative stage throughout the planning phase until they are deemed ready for execution.

Another aspect of MSE planning is the sheer volume of plans needed to meet the diverse security requirements. Because of this, it is helpful to categorize plans that have a common purpose in groups or categories. These plan categories are complementary and interdependent in terms of their operational intent. Categories of plans provide for a systematic management approach that helps ensure interoperability, gap analysis, and more effective use of resources. Government policy, economic pressures, geographic realities or threat levels influence how planners categorize plans. For the purpose of this chapter, we categorise plans using the following headings:

- **Operations Plans**: the more tactical plans, designed to protect or secure particular areas such as venues and non-venues. They also include specialized plans that have a specific functional requirement such as Cybersecurity, Transportation, Accreditation, Public Order, and Counter-Terrorism;
- **Support Plans:** designed to provide the appropriate logistics and resources so that operations plans can be executed. Support Plans may include, but are not limited to, private security, communications, logistics, mobilization of human resources, knowledge transfer, information technology;
- **Contingency Plans:** designed to manage modifications or adjustments to safety and security during the event period or the implementing stage. They are supplementary to the operations and support plans.
- **Master Security Plan:** a combination of the various categories of plans. The master security plan should also become part of the larger MSE Event Plan.

## 2.2 Three-Stage Process

The following is a three-stage process that describes how plans evolve from Stage One (basic state) to Stage Two (the validation process) to Stage Three (confirmation exercises). This process will bring the plans to a “state of readiness” for execution during the operational phase.

### *2.2.1 Stage One (Basic State)*

In this stage, planning practitioners work collectively to build their respective plans as they relate to their organization’s role in the overall security framework. In so doing, planners align their activities to support the mission-critical objectives and the mission’s core values. At this time, the plans are in a formative or basic state, having not undergone an interagency validation process (See Diagram 6 below).

For demonstration purposes, some of the more consequential plans are listed here, using the same categories as listed in Diagram 8, namely Operations Plans, Support Plans, and Contingency Plans. As one works through the plan development process, the plan’s interdependencies will become more apparent.

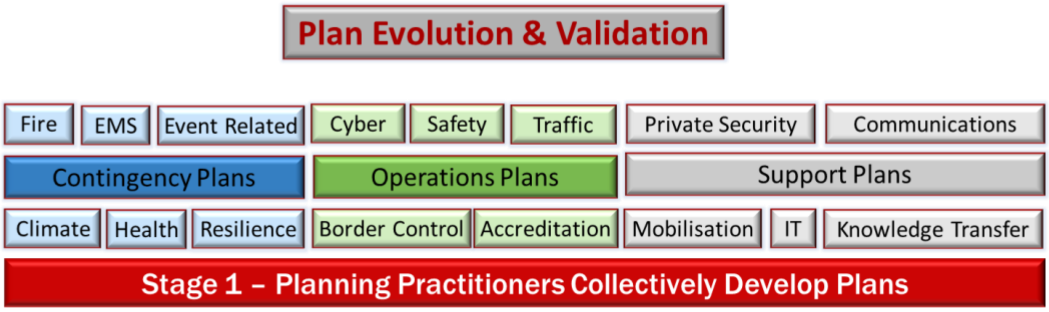


***Diagram 6. - A visual representation of Stage One or Basic State. It identifies some of the planning subjects associated with the three planning categories. The plans listed under these headings represent a larger volume of plans related to each category.***

### *a. Operations Plans*

Operations plans must be flexible enough to allow public access to all venues to participate as spectators in the MSE while at the same time apply adequate security measures to protect both athletes and public from anyone intending to cause disruption, harm or terror in the community. They should be broad in scope and include air, land, and marine components and focus on deterrence and intervention to inhibit malicious acts meant to cause severe harm or injury to people and destruction of property. As mentioned, these plans must be based on program requirements and threat risk assessments (TRA).

The following is a list of some of the more prominent considerations to be taken into account when developing operations plans at the Basic Stage.

- Transportation and Traffic Management

The predominantly open and widely unprotected network of public transport systems makes these attractive targets for criminals and terrorists. A major attack on one area of the transportation system could, in a worst-case scenario, shut down the entire network, impacting on the MSE whether the actual venues are targeted or not.

**Vehicle traffic management** is one of the elements associated with MSEs that are commonly scrutinized. Traffic congestion, detours, and road closures are often attributed to the MSE because of the large volume of spectators and the burden for supporting infrastructures accompanying the event. Security planners must work with transportation officials, traffic engineers, public utilities, fire-emergency medical services, and others, to ensure that spectators, businesses and the community at large experience only minimal disruption in their daily lives during the event. Decisions to close streets and stop transit temporarily, re-routing traffic, or to change the regular local routines may be made for safety or security reasons. It is paramount that the impact caused by these adjustments be proportionate and last only as long as really needed.

It is recommended that planners consider creating:

- dedicated event lanes on the roadways;
- material loading and unloading stations with sufficient security screening areas, on-bussing and de-bussing zones; and
- spectator vehicle parking areas away from the venues from which ticket holders can be pre-screened and bussed into the venue.

The business sector can also assist with transportation security planning, as many private companies have honed and professional safety and security infrastructures that can be utilized in support of the larger MSE security framework. Companies can be effective security partners and should be considered for inclusion in the joint working groups whenever appropriate.

- Cybersecurity

As organizers rely heavily on technology to deliver a successful event, critical information infrastructure and other cyber-empowered networks are particularly vulnerable to various forms of attacks originating from both State and non-State actors. Accordingly, a broad cyber-defence strategy needs to be put in place (see Chapter V on *Legal and Institutional Frameworks*).

The MSE cybersecurity defence plan should complement and make maximum use of existing national cybersecurity agency structures and international partnerships against cybercrimes. The MSE's integrated cybersecurity team should be composed of trusted government and private-sector security specialists of Information Management Information Technology (IMIT) as well as law enforcement investigators. Together, they need to develop and implement a comprehensive plan to deal with cyberattacks, based on "detect, respond and recover" capabilities. Such a plan should include a defence mechanism for computers, servers, mobile devices, electronic systems as well as other network components.

- Accreditation

Accreditation can be viewed as one cornerstone of security and the first line of defence. It is vital that Government officials, the Local Organizing Committee, business-sector partners and participants have a good understanding of the impact that shortcomings or breakdowns in the accreditation process can have for the MSE’s success or failure. It can even affect the host country’s international reputation long after the major sporting event is over, if accreditation mistakes occur beyond the occasional glitch.

The purpose of accreditation is to identify persons and their roles at the MSE and provide them with the necessary access to perform their roles. Accreditation is not a sign of privilege or status; it is an essential working tool to manage the large numbers of individuals participating in sporting events and to facilitate their movements in a secure but also flexible way.

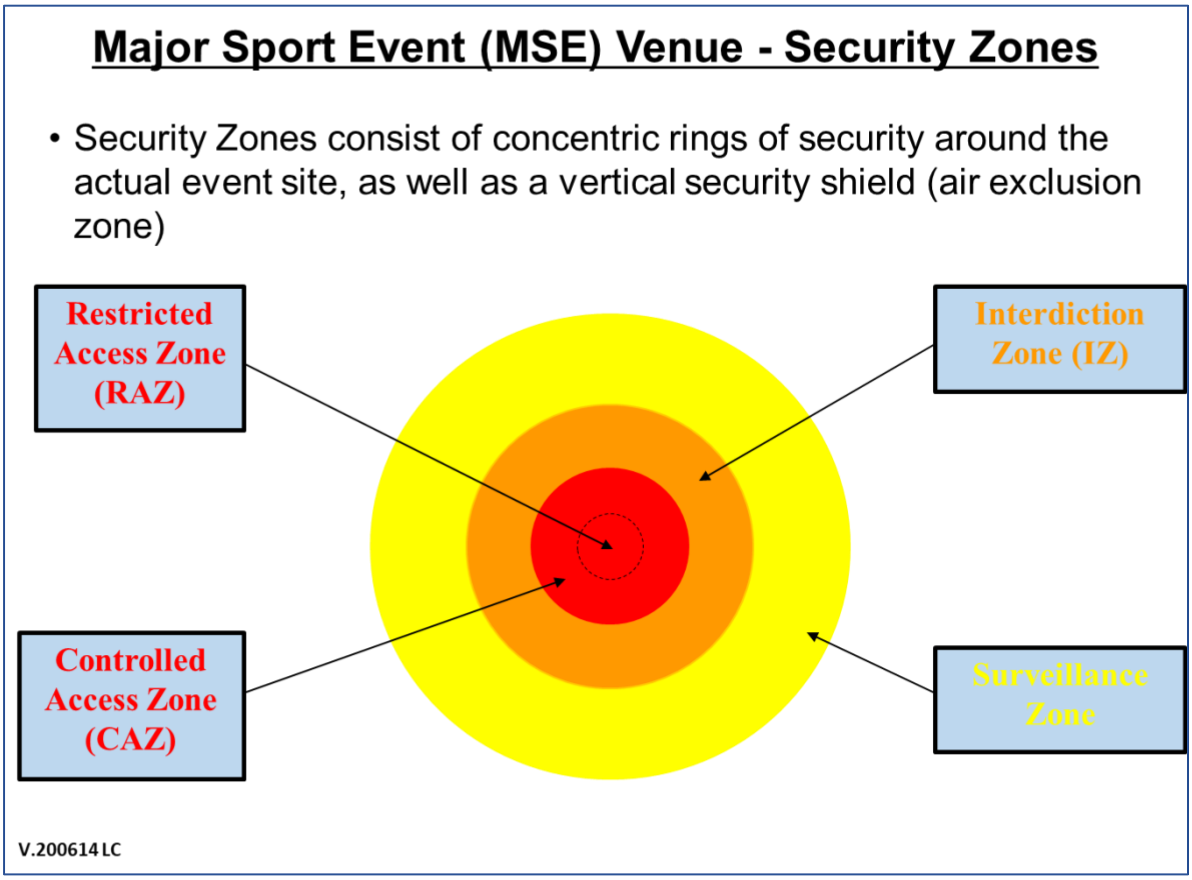
Accreditation:

- Ensures that only properly qualified and eligible persons are entitled to participate in the MSE or perform official tasks and functions;
- Limits individuals to access only the areas they need to go to perform their official functions and keeps unauthorized individuals out of secure and operational zones; and
- Safeguards against security risks by conducting a background check on all individuals who apply.

The accreditation process provides a framework to ensure that accreditation applications are completed accurately, that persons requiring accreditation are properly screened by means of a law enforcement security background check, and that unauthorized people do not receive accreditation. The platforms used within the accreditation process include the access credentials (Identification Card) which are often interfaced with many of the MSE logistical functions. In addition to granting access rights, the credentials are usually barcode-referenced and can be used for obtaining meals, accommodation and transportation. Security features are built into the ID cards such as Radio Frequency ID (RFID), biometric recognition, Bluetooth low-energy beacons and GPS technology.

### • Venue and Non-Venue Security

A layered approach should be considered for the protection of MSE venues.



Major Sport Event (MSE) Venue - Security Zones

- Security Zones consist of concentric rings of security around the actual event site, as well as a vertical security shield (air exclusion zone)

Restricted Access Zone (RAZ)

Interdiction Zone (IZ)

Controlled Access Zone (CAZ)

Surveillance Zone

V.200614 LC

*Diagram 7: 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*

Diagram 7 above explains the protection layers and the type of security protection coverage that each layer offers for an MSE venue. Strategically positioned police and private security personnel should be deployed within the venue and the outer-venue perimeter in accordance with their assigned duties and responsibilities to ensure security protection coverage.

- **The Restricted Access Zone (RAZ):** refers to the Field of Play to which only qualified people have access, such as field-maintenance crews, television/media, game and field officials, referees, medical doctors, first aid teams, players, athletes, and security personnel. It also includes the players' or athletes' changing rooms and medical facilities, and maintenance crew areas. The access to this area should be highly restricted.
- **The Controlled Access Zone (CAZ):** refers to the inner perimeter, which includes the stadium seating area and the areas within the stadium where vendors and restaurants can be found. The event overlay usually expands the actual venue site significantly to

account for radio broadcast and TV media space as well as sponsor activities. Vehicle Screening Area (VSA) and Pedestrian Screening Area (PSA) screenings should be conducted prior to any vehicles (service, team or official) or pedestrians entering the CAZ. The security responsibilities within this zone include protection of life, ensuring the prevention of equipment sabotage, and the deterrence of any adverse misbehaviour or other threat within the venue footprint.

- **The Interdiction Zone (IZ):** refers to the immediate surroundings of the stadium venue or the outer perimeter. The primary task of the security personnel would be to ensure proper crowd management and interdiction of any criminal activity.
- **The Surveillance Zone:** is the public domain area outside of the Interdiction Zone. The primary task of personnel deployed in that zone is to conduct regular policing and public-safety activities while also monitoring, identifying, and responding to any unusual or suspicious activity that could interfere with the smooth conduct of the event.

### • Deployment and Use of Surveillance Equipment

Human resources deployments should be complemented by strategically installed Perimeter Intrusion Devices and 360-degree CCTV camera systems, allowing for real-time surveillance and intrusion monitoring. As highlighted in chapters V and VI on Legal and Institutional Frameworks and on Stakeholder Cooperation, deployment and use of surveillance equipment always need to take due consideration of their potential impact on human rights, particularly in the light of applicable data protection legislation and the right to privacy. Planners should consider exploring opportunities for public-private partnerships for the procurement and deployment of surveillance equipment. Technology companies often have affiliations with the ISFs or LOCs and arrangements for Value in Kind (ViK) sponsorships can be negotiated when public procurement regulations permit.

### • Border Control

MSE security planners must ensure that this operations-plan component includes a direct link to the national border services and immigration authorities. Ensuring effective border security is an integral part of any comprehensive and integrated national counter-terrorism strategy and requires collective action by States and relevant international and regional organizations. For example, Coordinated Border Management (CBM) strategies, which require close coordination among the competent authorities at border locations, have in many cases proven to be a highly effective tool for managing national borders.

### *b. Support Plans*

During Stage One (Basic State), support plans are to be designed with the aim of outlining the appropriate logistics and resources so that Operations plans can be executed. Support Plans may include but are not limited to, private security, communications, logistics, mobilization of human resources, knowledge transfer, information technology, etc.

#### • Role of Private Security

It has become a common occurrence to see private security personnel perform certain specific duties at MSEs around the world, under the supervision of the major event lead police agency. The use of private security, complementing the functions of the lead police agency and their police and military security partners, has proven to be successful. It allows official security forces to focus on their core security mandates and provides more efficient security coverage during an event.[92] Private security officers, as well as the Stewards and Security Volunteers, become “force multipliers” in support of the MSE Safety and Security mandate.

However, to ensure full synchronization between private security agencies and the lead police agency, several components must be considered:

- Private security personnel must be hired at least six months before the beginning of the MSE, and security background checks must be completed on each candidate before hiring;
- Private security personnel should receive appropriate and thorough training and certification for performing their duties;
- Private security personnel must participate in “dry-run exercises” or in test events leading up to the MSE under the supervisory oversight of the lead police agency;
- Private security personnel must remain under contract for the duration of the MSE. The contract should have enough incentives to ensure that private security personnel does not leave for the highest bidder searching at the last possible moment for additional event staff. Duration bonuses could be an incentive to retain temporary staff.

[92] Addressing the role of private security companies within security sector reform programmes; see https://www.files.ethz.ch/isn/39540/PSC_report.pdf .

- Private security personnel should be included in the contingency planning, where specific actions of their security personnel are incorporated.

- Communication and Social Media Strategies

As also highlighted in Chapters VI on Stakeholder Cooperation and in Chapter VIII on Communication Strategies, a strong Communication Strategy is critical to the success of an MSE. The objective of this strategy should be to build and maintain public confidence in the security measures, to engage in transparent and timely interactions with the media, while protecting the integrity of the security operations, and to provide timely communications both internally and externally.

It is recommended to create an Integrated Security Communication Team (ISCT) with the responsibility of sharing information and addressing communication/media issues that may affect the security of the MSE. The ISCT should develop and implement a coordinated and integrated external communications and social media strategy to convey a clear, transparent, timely, consistent and coordinated messaging to all involved and impacted by the MSE.

- Information Management Information Technology (IMIT)

The magnitude, complexity and fluid nature of MSE planning demands that there be a robust and secure data management and transmission platform in place. The ongoing data revolution requires that the MSE's partners have a modern, reliable, interoperable and accessible IMIT environment that allows for collaborative and secure sharing of information and data. The platform to be used should be introduced at the beginning of the planning process and be agile enough to receive security upgrades in the course of the multi-year planning cycle. The platform must have protective capability measures with a focus on safeguarding sensitive data, layered defences to reduce exposure to the cyberthreats mentioned earlier in this chapter, and also possess a user-friendly education component with an emphasis on increased security awareness.

### *c. Contingency Plans*

Contingency plans are required for simple changes to event schedules as well as for handling more dynamic situations such as potential high-risk safety or security events such as fires, extreme weather conditions, natural disasters or health hazards and disease epidemics.

Contingency plans should have a comprehensive "all-hazards" approach that ensures a coordinated and organized response to any emergency that might happen during the event. Security planners need to design not only robust integrated contingency plans but make sure that there are management systems built to execute and control effective responses. Business continuity and resiliency must be considered in all contingency plans. Below are two examples of some of the subject areas that require contingency plans to take into consideration.

- Health Contingency Plans

Global health concerns have been prevalent during the planning and operations of many MSEs. The fast-mutating global spread of the H5N1(Avian bird flu) in 2006 prior to the Torino Winter Olympics in Italy; the Zika virus epidemic prior to the 2016 Rio Olympics in Brazil; and the COVID-19 (Coronavirus) pandemic causing the postponement of the 2020 Japan Summer Olympics are all examples of health concerns that have impacted on MSEs. Spectators, athletes, and the entire MSE workforce could be negatively affected by several types of health concerns, ranging from localized food poisoning to a broader disease outbreak.

World Health Organization COVID-19 Recommendation (29 May 2020)

Any decision to restrict, modify, postpone, cancel or proceed with holding a mass gathering should be based on a rigorous risk assessment exercise, tailored to the event. The risk assessment should be undertaken by local and national public health authorities and event organizers with input from relevant authorities (emergencies, transport, safety and security, etc.), based on the following considerations:

- ✓ **The normative and epidemiological context in which the event takes place** – the host country's existing regulations on public health and social measures to control the spread of COVID-19, which reflects the intensity of transmission in the area.
- ✓ **Evaluation of risk factors associated with the event** – appraisal of the likelihood that the event may contribute to the spread of COVID-19 and that the health services capacity may be exceeded by such spread;
- ✓ **Capacity to apply prevention and control measures** – the ability to implement actions that can reduce the risks associated with the event.

The overall risk associated with a mass gathering event is the outcome of a process that incorporates (a) the risk of amplified COVID-19 transmission associated with the event, and it's expected burden on the health system and (b) the capacity of health authorities and event organizers to prevent and control such risks.[93]

Source: World Health Organization, Key planning recommendations for mass gatherings in the context of COVID-19, Interim guidance 29 May 2020; see https://www.who.int/publications/i/item/10665-332235 .

[93] World Health Organization, Key planning recommendations for mass gatherings in the context of COVID-19, Interim guidance 29 May 2020; see https://www.who.int/publications/i/item/10665-332235 .

- Safety Management Contingency Plans

Safety management is a universal responsibility shared by all participating stakeholders at MSEs. While the primary responsibility for safety at organized events, held inside or outside of stadiums, should rest with the principal event organizer, the role of national coordination arrangements is crucial in providing clear and unambiguous legislative and regulatory frameworks which empower and enables safety personnel to fulfil their obligations effectively. To that end, a national, multifaceted safety infrastructure should be designed and implemented so that:

- The legal, regulatory and administrative framework provides clarity on the roles and responsibilities of the organizer, stadium safety officers, police and other emergency services;
- The legal, regulatory and administrative framework obliges stadium safety officers (on behalf of the organizer and/or stadium management) to provide a safe stadium environment for all participants and spectators;
- Stadiums ought to provide an inclusive and welcoming environment for all communities and the people in general and incorporate, inter alia, the provision of appropriate sanitary and refreshment facilities along with good viewing arrangements for all spectators (including children, the elderly and disabled supporters); and
- The legal, regulatory and administrative framework provides clarity on respective roles and responsibilities of the municipal authorities, police, other emergency services and the organizer regarding events held in public places outside of stadiums.[94]

### *2.2.2 Stage Two (Plan Validation)*

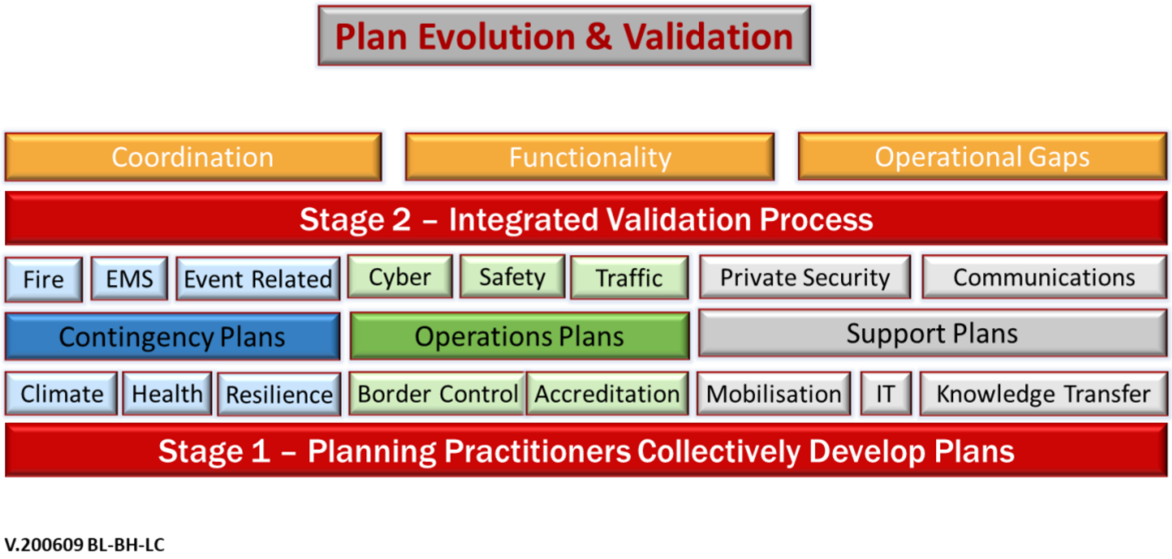
Until this point, planning has been at the formative or developmental stage where all stakeholders have been formulating plans based on the Mission Critical Objectives and the Organizational Core Values. As referenced earlier, this can amount to a considerable number of plans from multiple agencies. Plans in this basic state are at risk of developmental isolation; therefore, they must be validated, one with the other, to ensure their interdependent

[94] Recommendation 2015 (1) Council of Europe Standing Committee on Safety Security and Service at Football matches and other sports events. See https://www.coe.int/en/web/sport/recommendation-2015-1 .

requirements are linked. Stage Two advances the plans through a validation exercise to ensure they address their intended function, bring into focus their interdependencies, ensure effective use of resources, and identify any operational performance gaps. Plan validation is a structured process whereby planners participate in an integrated exercise designed to ensure plans are aligned and ready for the exercise testing in Stage Three.

**Diagram 8 - A visual representation of Stage One and Stage Two.**

**Stage Two represents the Integrated Validation Process that focuses on plan relationships in terms of Coordination, Functionality, and Operational Gaps.**



Plan Evolution & Validation

Coordination | Functionality | Operational Gaps

Stage 2 – Integrated Validation Process

Fire | EMS | Event Related | Cyber | Safety | Traffic | Private Security | Communications

Contingency Plans | Operations Plans | Support Plans

Climate | Health | Resilience | Border Control | Accreditation | Mobilisation | IT | Knowledge Transfer

Stage 1 – Planning Practitioners Collectively Develop Plans

V.200609 BL-BH-LC

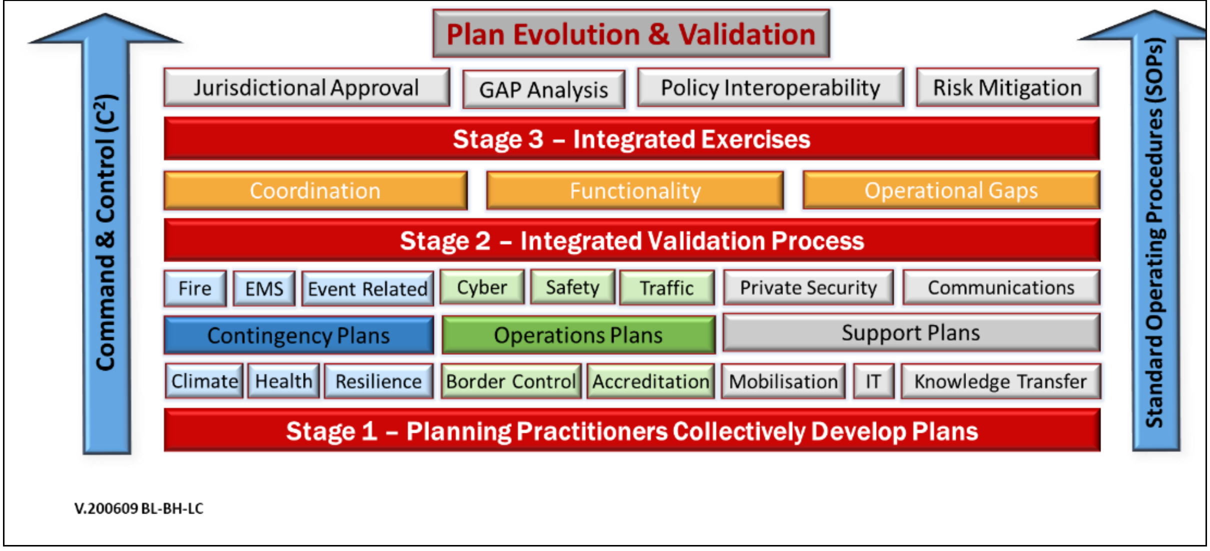
The validation process is an activity of the Joint Operational Planning Group (See Diagram 3 in Chapter VII). It aims to enable an integrated approach where planners collectively review their various plans and track their interdependent requirements. It allows planners to critique each other and make suggestions for improvement**.**

The validation process is co-dependent on the size of the event and may be repeated throughout the planning phase as security needs change. Experience has shown that an effective way to conduct the process is to review the plans by category, either in written form or by using presentation software. The presenter should explain which of the Mission Critical Objectives the plan supports, outline the human and material resource requirements, and make a note of any additional support needs.

Quite often, projected activities or proposed competition or non-competition venues presented during the MSE Bid phase do not materialize, and alternative solutions are delivered at the actual event time. The shift from the initially envisioned designs from the Bid to the final event delivery can have a significant impact on the budget, which was originally used to project the event security costs. Initial assumptions were made on the best-known information at the time; however, as the event program evolves and information becomes more accurate, the degree of change (per assumption) has to be tracked in terms of cost variance. This process enables those in charge of finance to specify how costs either increased or, less likely, decreased as the event evolved relative to the initial budgetary projections. As indicated earlier, this scope of work is separate from the plan validation process. However, the change variance tracking is using a similar method. For this reason, it could be a dual role, performed by the change control coordinator.

### *2.2.3 Stage Three or the Integrated Exercise Process (Testing State)*

**Diagram 9 : Stage Three, which is "Exercise"-focused and is the final requirement to be put in place before going into the operational phase.**

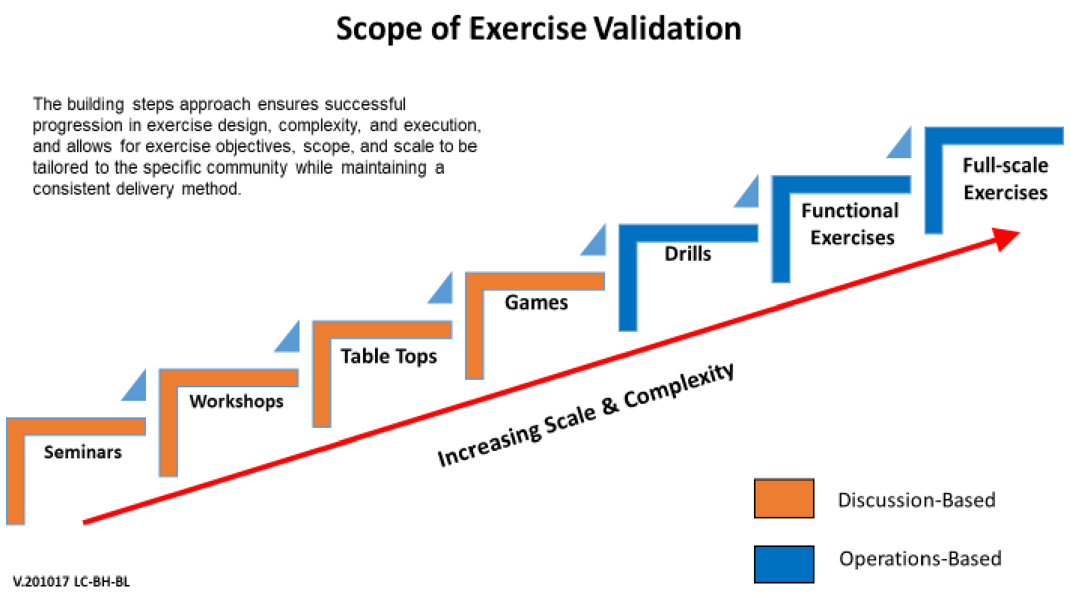


Once plans have undergone a validation process, they are ready for Stage Three, which is a test stage to determine the degree of operational readiness. An exercise program must be established early on with the aim to allow the practice and observation of relevant security and safety plans, operational procedures, command and control and intelligence processes as well as government-wide information management.

The planning cycle for each exercise (Tabletop exercise – TTX or Functional Exercise) can include the following activities:

- Initial Meeting: to determine exercise scope.
- Follow-up Meetings: to discuss exercise organization and staffing concepts, scenario and timeline development, scheduling, logistics, and administrative requirements.
- Writing Board Meetings: to develop a list of actions, in chronological order, that supplement the exercise scenario with information - such as event synopses, expected participant responses, objectives and core capability targets to be addressed, and responsible personnel.

**Diagram 10 - Represents a building-block approach to validation and test exercising**



The building steps approach ensures successful progression in exercise design, complexity, and execution, and allows for exercise objectives, scope, and scale to be tailored to the specific community while maintaining a consistent delivery method.

The building-block approach to validation and test exercising ensures successful progression in exercise design, complexity, and execution. It allows for exercise objectives, scope, and scale to be tailored to the specific community while maintaining a consistent delivery method.

As highlighted throughout this Guide, security is a massive undertaking that not only involves those with security-specific mandates but also corporate partners. Throughout Stage Three, a series of *tabletop exercises to test the plans* should be held at different levels within the security hierarchy. All testing exercises should be designed with specific objectives in mind to validate plan requirements such as to:

- Confirm processes and procedures, as well as the mechanisms for providing shared situational awareness to provide an integrated response to threats or emergencies.
- Confirm security command/coordination and control arrangements, as well as information sharing and decision-making processes in support of the MSE.
- Confirm the sharing of information internally and externally between security officials and jurisdictional partners (See Command and Control Concept of Operations Section 2.2.4 on *Final Stage*).
- Confirm the plans and processes for the allocation of specialized resources within and across jurisdictional lines (Policy Interoperability, Jurisdictional Approval).
- Test and practice the integrity and interoperability of communications networks and information systems
- Ensure that plan gaps are identified and closed.
- Ensure that plans have been assessed in terms of risk, and established mitigation strategies are adequate.

### *2.2.4 Final Stage (State of Readiness)*

Until this point, this Guide has been addressing activities critical to the planning process. Once the plans are validated and tested, and the organizers are satisfied that they have met the objectives of the exercise, the plans are deemed ready to be operationalized or executed.

However, before a "state of readiness" can be declared, there are two remaining critical elements required to operationalize the plans. The Command and Control Concept of Operations (C2ConOps) and Standard Operating Procedures (SoPs) represented by the blue arrows in Diagram 10 above are the final elements of the plan evolution process. There will be a requirement to create a C2ConOps and SoPs at the final stage, as described below.

- Command and Control Concept of Operations (C2ConOps)

To achieve effective collaboration in an integrated environment, all partners must understand each other's policies and directives before entering into the operational phase. Even though the plans have evolved through a three-stage process and been deemed operationally ready, they are still just “plans”. What is required is a process that recognizes and acknowledges organizational, cultural, and technological differences as a means to conduct integrated operations and thereby execute the by now interoperable plans.

This process is set out in a C2ConOps document formulated by those security entities who have jurisdictional authority over event operations. Internationally, there are various command structures; therefore, no single process is being suggested in this Guide. The focus here is on the importance of the creation of a hierarchically organized command document that satisfies operational security requirements and identifies decision-making authorities. The production of this document must commence in Stage One and evolve to Stage Three, not unlike the other categories of plans. This evolution process is visualized in Diagram 9 by one of the vertical blue arrows that overlay the three-stage process. It represents the implementation of the agreed-upon system that coordinates plan execution, based on the event operational environment.

- Standard Operating Procedures (SOPs)

Standard Operating Procedures (SOPs) are detailed, written instructions on how staff should perform a routine activity. Easy-to-read SOPs explain every detail of a process. It is essential to understand that a good SOP does not focus on what needs to be done, but rather on *how* it should be done. It is critically important that every venue and non-venue manager establish site-specific SOPs, makes sure that staff review these SOPs, and ensure that they are visible.

Examples of SOPs

✓ Arrest and release procedures
✓ Site safety procedures
✓ Site-specific operating procedures
✓ Managing drunk and disorderly people
✓ Reporting of stolen property
✓ Safeguarding a crime-scene
✓ Lost passports
✓ VIP protocols
✓ Athlete Management Issues
✓ Asylum seekers
✓ Spotter protocols

## 3. Post-Event Evaluation and Knowledge Transfer

At the end of an MSE, there are two crucial steps for organizers which can be influential far beyond the life of the event itself. A Post-Event Evaluation is crucial to the evolution and improvement of future events through analysing the success and value of strategies used. In addition, the action of Knowledge Transfer can be of vital importance to future event planners.

- **Post-Event Evaluation**

The Post-Event Evaluation should encompass an assessment of which expected outcomes were achieved and to what degree, alongside the value, failure and success of the strategies or processes which were utilized during the life of the MSE, enabling important lessons to be learned and best practice to be identified.

The evaluation is of benefit for those planners required to report to Governments and sponsors who have provided funding or material assets to support certain security planning requirements. The prevailing question in this methodology is "Was it worth it?", which can be asked in terms of the value of certain planning strategies, which incidentally, is also of use to future planners. A key focus of this evaluation is on "good value for money" and whether the activities and strategies were time efficient. Hosting Authorities should be aware that this is an essential part of engaging private-sector service providers and the Government whose concern it is to balance cost and benefits.

To achieve this, Post-Event Evaluation involves the use of logic models, input-output analysis and other methods to gauge the degree of value. Therefore, to attain a valuable outcome from an evaluation, a methodology based on the analysis of system inputs and their expected outputs is needed to be understood from the outset. Expertise in evaluation processes in terms of data analysis is essential for the team designated to lead the evaluation process.

- **Knowledge Transfer and After-Action Reports**

Separate from the Post-Event Evaluation methodology is the production of Knowledge Transfer and After-Action Reports.

An organized and effective transfer of knowledge plan identifies, captures and communicates key insights gained from the entire MSE project, so that future MSE planners can reduce risk and costs based on lessons learned. Without this kind of information, future planners risk repeating costly mistakes.

As already mentioned in Chapter VI on *Stakeholder Cooperation*, the Post-Event Evaluations and After-Action Reports also represent an important opportunity to produce legacy materials which can be shared with prospective future Host Authorities. In some cases, sports federations produce reports that document critical issues and outcomes of specific events, along with recommendations, that can be used for future events or shared with law enforcement agencies, other sport disciplines, major event organizers, health authorities or private-sector partners.

A good working example of this is the IOC Olympic Games Knowledge Management (OGKM) program which provides an integrated platform of services and documentation, assisting new organisers in their Games preparations, while also facilitating the transfer of knowledge from one Organizing Committee (OCOG) to another. The OGKM programme consists of three main parts: information, services, and personal experience, along with Official Games Reports, technical manuals, knowledge reports, and a range of other useful documents and publications that are all available on a dedicated extranet which Organizing Committees are able to call upon throughout their lifecycle.[95]

## Recommendations

## The security planning

### General principles and governance

→ Understand security planning as a prerequisite to ensure that operations become executable, sports competitions take place without disruptions, and the experience is positive for all present. At the same time, ensure that security complement, as opposed to hinder, the overall event experience.

→ Ensure that authorities in charge of security define their vision for the security operation in line with the overall mission and strategy for the MSE. All contributors should understand and adhere to that vision.

→ Plan for security as a "whole of government" effort, beginning as early as possible and broadly involving all stakeholders with roles and responsibilities in the security domain, including the MSEs' local organizing committee and the business sector.

[95] "Olympic Games Knowledge Management Programme Provides 'Essential' Resource For Games Organisers," *International Olympic Committee*, 22 Feb. 2014; see https://www.olympic.org/news/olympic-games-knowledge-management-programme-provides-essential-resource-for-games-organisers.

→ Ensure that one Ministry act as the Government's lead security agency responsible for the MSE.

→ Ensure that the security planning system bring together multiple agencies with diverse backgrounds and engage them at various levels as executive leaders, senior leaders, mid-level managers and tactical planners.

**Leadership**

→ Ensure that security leaders are prepared to embrace and build trusted relationships and take a conciliatory approach when dealing with competing or conflicting issues.

→ Recruit a lead security planner with strong experience in strategic planning, risk and project management.

**Strategic approaches to security planning**

→ Ensure that the level of visibility of the security apparatus - although discreet - remains noticeable by attendees, acting both as a deterrent against possible malicious acts and conveying a sense of protection.

→ Develop adaptable and scalable security plans (up/down in terms of scope and resources) to respond to a fluid an evolving threat landscape in the course of the planning phase.

→ Plan for worst-case scenarios (e.g. terrorist attacks, violent protests, natural disasters such as earthquakes) in the framework of an "all-hazards" approach, while also preparing for more likely ordinary crime situations and incidents.

→ Throughout the planning cycle, subject security plans to testing and validation with robust exercises in order to declare a state of operational preparedness.

→ Categorize plans into groups, which allow for a systematic management approach to ensure interoperability and ensure more effective use of resources as plans evolve.

→ Consider a layered approach for the protection of MSE venues and other sites.

→ Run a "Knowledge Transfer Process" from the very start of the planning phase as a way to capture key insights gained from the entire MSE project, so that future planners can reduce risk and costs based on lessons learned.

**Security Design**

→ Design security from the start, based on international standards and best practices, in order to prevent costly redesign or ineffective security solutions

→ Approach the security design as a multidisciplinary endeavour, with security designers liaising with architects, landscape architects, mechanical-electrical-plumbing MEP engineers, ICT engineers, fire and life safety (FLS), crowd modelling, transport modellers, lighting engineers etc.

→ Designs should be agreed upon at each stage before the security design is undertaken so that the need for redesign is minimized.

**Planning for resource management**

→ Use existing infrastructure and equipment to the greatest possible extent to reduce costs and procurement delays.

→ Facilitate opportunities for "joint procurement", i.e. when multiple LOC or government entities may require the same good or service (e.g. acquisition of hotel rooms or hospitality requirements)

→ Ensure that the integrated multi-organizational security system has a built-in mechanism to ensure that plans are interoperable.

→ Consider involving law enforcement entities such as the coast guard, park rangers, conservation officers, fisheries' officers or any other capable professional national/regional/local law enforcement officials to enhance security and create a force-multiplying effect.

→ Consider utilizing professional and well-trained private security personnel as an official security force multiplier and as a tool to create cost efficiencies.

# VIII. COMMUNICATION STRATEGIES

A strong internal and external communication strategy related to security is critical to the success of an MSE. The objective should be to build and maintain public confidence in the security measures, to engage in transparent and timely interactions with the media and other external stakeholders, while protecting the integrity of the security operations, and to provide timely communications, both internally and externally.

## 1. *Effective Communication with MSE Security Stakeholders*

Strategies that produce effective communication with stakeholders are generally established around six core benchmarks:[96]

- ✓ **Accessible:** Stakeholders must be able to access the information they need to make informed decisions and fulfil their respective roles in security planning and operations. Organizers should identify all channels that are available and map their capacities to reach priority audiences.
- ✓ **Credible and trusted**: Building an open and transparent environment to facilitate cooperation among stakeholders is critical to ensure stakeholders undertake appropriate measures to support security operations. Organizers need to demonstrate competence, dependability, and willingness to engage stakeholders early and often.
- ✓ **Timely:** Organizers must communicate in a manner that ensures stakeholders feel included in the process and allows them the time to make informed decisions and take appropriate action.
- ✓ **Actionable:** To be successful, organizers must understand their audiences' knowledge, attitudes, and behaviours in order to create messages that address barriers and encourage decision-makers to take the recommended steps.
- ✓ **Relevant:** Effective communications need to be useful and helpful to their target audience.
- ✓ **Understandable:** The various stakeholders involved in security planning will have different areas of expertise and levels of technical knowledge. Host organizers must ensure that communications be tailored to specific audiences, and that information be precise, understandable, and clearly convey the action you want the audience to take.

[96] World Health Organization. *WHO Strategic Communications Framework for Effective Communications.* 2017, see https://www.who.int/mediacentre/communication-framework.pdf?ua=1.

| Effective Communication Strategies |
|---|
| ✓ Supporter organizations are a direct channel to disseminate security protocol information to fans who plan to attend the event.<br>✓ As part of the planning exercise, organizers will be working to encourage partners to adopt certain activities or behaviours to support event security.<br>✓ Partners from international Governments might not need to be told details of venue security; however, they would need to be informed about risks that could impact them at a national level (e.g., safety and security of their participating athletes, secondment of police forces, etc.). Similarly, security operations may include emergency management, public health, transportation, public works, and the private sector, but not every stakeholder will need the same level of detail. |

### 2. *Internal Communication Strategies*

As set out above, effective internal communications will set the stage for proper and professional external communications when it comes to security matters. In addition to communications experts who would be located within the LOC (but generally will be tasked on external communications), it is recommended that an Integrated Security Communication Team (ISCT) be created with the responsibility of sharing information and addressing communication/media issues that may affect the security of the MSE. The ISCT should develop and implement a coordinated and integrated external communications and social media strategy to convey a clear, transparent, timely, consistent and coordinated messaging to all involved and impacted by the MSE.

The following are some considerations to be taken into account by the Integrated Security Communication Team:

- Establish and maintain an open dialogue with the public, the business community, activist groups and the media to address concerns and work together towards a peaceful and safe MSE. The promotion of partnership among the participating security, government, organizing committees, stadium event planners, and corporate partners for the MSE is critical.
- Take full advantage of the Internet and social media to inform all stakeholders, including the public, about the security measures in place and how these will affect them (e.g. road closures and event dedicated roads, special public transportation measures).

- Use tools to monitor social media trending that can supply situational awareness of current events, forward findings to an event-specific Unified Command Centre, and take appropriate action. Web exchanges in social media allow interpretation of the public mood and, can, to some extent, even predict people's likely behaviours in certain situations. By leveraging social media, planners can gain greater situational awareness and enhance communication strategies. Social media monitoring should always be conducted within the confines of the law and with due respect for existing privacy regulations.

### 3. *External Communication Strategies*

#### a. Communication with the Public

A strategy to communicate with the public is paramount during all stages of the MSE life cycle, i.e.:

- during the Exploratory and Bidding Phases it should help to create momentum, enthusiasm, engagement and a common sense of purpose within the community;
- during the Planning Phase it should maintain momentum, popular and political support, and create transparency as to how public resources are being used;
- during the Implementation Phase, a good external communication strategy should keep spectators and staff properly informed, which can also contribute to better surveillance and detection of threats; and
- during the Post-event Phase, it should communicate the positive impacts of the MSE on the community and host authorities.

#### b. Community Relations Group

Intrinsic to proper public engagement and also one of the most important elements to be considered in the communication strategy is the creation of a Community Relations Group (CRG), mandated to establish and maintain open and transparent lines of communication with all stakeholders who may be affected, directly or indirectly, by the preparations for the MSE (e.g. local business operators and community residents). Establishing mechanisms for consultation and collaboration with these groups can help improve specific aspects of security planning and operations - e.g., local groups dedicated to special issues such as youth radicalization and prevention of violent extremism. This can enhance understanding of the local context and provide information which might be useful in security planning. In the safety field, local communities are also a source of knowledge on vulnerable people or persons with disabilities who should be considered during crowd management or at security checkpoints.

### c. Communication with other External Stakeholders

Another key part of communication with the public involves all relevant stakeholders as trusted partners in the security system. In practice, this means that:

- Security Planners need to be both informed and consulted about decisions, thus creating two-way communication.
- Organizing committees, government agencies, and business-sector entities have to become involved in the decision-making process regarding security issues.

### d. Media Engagement

The media have the ability to influence public perception of the security process positively or negatively. There must be a strategy to keep the media informed of relevant information impacting the broader public interest. A plan to directly engage the local media and the public to address concerns as to how the event might affect the local community must be made and implemented. An example of this was the communication of the security strategy for the London 2012 Olympic Games in which a picture of a battleship on the River Thames equipped with missile launchers became a symbol of the security operation for the Games. With more thorough media engagement and a better communications plan, this military display could have been packaged in a more positive way.

### e. Social Media

Social media have become a powerful tool for reaching diverse audiences, including when it comes to conveying security measures. Furthermore, through frequent communication on social media platforms, the LOC can maintain a constant dialogue with the public, and thereby can build trust in the community, which in turn enhances security.

## Recommendations:

### Communication strategies

→ Design a strong internal and external communication strategy aimed at a) building and maintaining public confidence in the security measures, b) engaging in transparent and timely interactions with the media and other external stakeholders; and c) providing timely communications, both internally and externally.

→ Set up an Integrated Security Communication Team (ISCT) with the responsibility of sharing information and addressing communication/media issues that may affect the security of the MSE.

→ Channel all requests for external communications through the ISCT to ensure consistency and avoid conflicting messages.

→ Develop a strategy to communicate with the public audience during all stages of the MSE life cycle as well as the planning phase.

→ Set up a Community Relations Group (CRG) in charge of establishing and maintaining open and transparent lines of communication with all stakeholders who may be affected, directly or indirectly, by the preparations for the MSE (e.g. local business operators and community residents).

→ Create a Community Activist Liaison (CAL) to ensure that there is an ongoing dialogue with activists and that their right to protest is acknowledged while being informed of police expectations, actions and consequences. CALs can be used to help enforce designated, agreed-upon protest areas.

→ Keep the media abreast of facts and situations impacting the broader public interest.

→ Plan to directly engage local media and the public to address concerns as to how the event might affect the local community.

# IX. SECURITY IMPLICATIONS OF CO-HOSTING MAJOR SPORTING EVENTS

Over the last 20 years, there has been a growing trend towards co-hosting international sporting events. MSEs have been organized bilaterally, such as EURO 2012, which was hosted by Poland and Ukraine, or they may involve multiple hosts - e.g. EURO 2020 was scheduled to take place across 12 European countries. In 2019, the Olympic Charter, which had previously restricted Olympic activities to one Host country, was revised to allow Olympic events to be held across multiple cities, regions, or even shared between adjacent countries.

As a result of global economic challenges, as well as the increasingly complex nature of MSE security -- including cost; personnel; the rising influence of transnational, public, and private partnerships; and the perceived threat of terrorism -- co-hosting can help to mitigate risks and reduce costs, ensuring secure and sustainable events. Partnerships can provide greater opportunities for prospective hosts, particularly for smaller countries that could otherwise not shoulder alone the financial burden and build the operational facilities required for such large-scale events.

## 1. Set up joint preparations well in advance, including the establishment of agreements between Governments and relevant multinational working groups

In the early stages of preparations, agreements between Host countries should be established to permit the closest possible cooperation. These agreements should address the development of a joint organization and planning strategy, the establishment of transparent organisational structures, the exchange of comprehensive information and data, the secondment of experts, and measures referring to safety and security. These agreements should be in addition to other formal or *ad hoc* security arrangements (e.g., for border security, police information exchange, or airspace security) with neighbouring, transit, or participating countries.

As an example, in 2008 the Government of Poland and the Cabinet of Ministers of Ukraine signed an agreement for cooperation for the organisation of EURO 2012, including the planning of safety and security. In 2010, a Polish-Ukrainian Road Map was signed, which clearly defined areas of cooperation in the preparation of EURO 2012. These included transport links (air, road, and rail), coordination in the field of information safety and the coordination of medical support.[97]

Safety and security working groups can help partnering countries to develop common or similar safety and security standards, provide compatible planning, management, and training of operational staff, and establish channels for the proper exchange of information.

For example:

- For EURO 2020, all 12 Host nations were required to present a safety and security strategy, based on a template outlining basic security requirements set by UEFA. While not every country is expected to achieve the highest security standards, this ensures every Host Authority will meet the minimum standards established by UEFA.
- The Council of Europe's Standing Committee of the Convention on Spectator Violence established, in 2016, an Ad-Hoc Working Group to monitor the safety, security and service preparations for UEFA EURO 2020. This Group met every semester since then and adopted a programme of consultative visits and peer-review exercises between match police commanders, which were carried out in half of the 12 hosting countries, notably: Azerbaijan, Hungary, Spain, Italy, the United Kingdom and the Netherlands[98].
- The Sports Grounds Safety Authority (SGSA) and the European Stadium and Safety Management Association (ESSMA) signed in 2020 an agreement to support the further development of safety and security of football stadiums across Europe. The agreement includes joint working areas in fan engagement on safety and security and the development, co-hosting, and accreditation of safety-related training modules, based on specifically created guidance documents.[99]
- CEPOL, the agency dedicated to training law enforcement in the EU, offers a Pan-European Football Security Course.[100] The course, which is designed to enhance the effectiveness and harmonization of the policing of football matches with an

[97] Liedel, K., and Piasecka, P. (2012). EURO 2012 Security as a Joint Task of Poland and Ukraine – A Challenge for National and International Security Systems. *Polish-Ukrainian Bulletin,* pp. 41-54.

[98] Council of Europe: Holding monitoring visits to ensure compliance with commitments by Member States

[99] See https://sgsa.org.uk/promoting-safety-across-europe/ .

[100] See https://www.cepol.europa.eu/education-training/what-we-teach/residential-activities/612020-pan-european-football-security .

international dimension within Europe, is offered to police football commanders, National Football Information Point contacts, football intelligence officers, spotters, and monitors.

### 2. Develop a clear overall police strategy and coordination structure

Establishing a plausible operations philosophy, based on risk assessments and the anticipated behaviour of fans, and the means to create close international police cooperation and information exchange is highly recommended.

While most security preparations and operations for in-country events will be carried out by local authorities within the Host country, there should be some level of collaboration with co-host nations and beyond.

For example:

- Co-hosting countries are encouraged to establish common standards of police acceptance levels (i.e., so fans can expect similar restrictions in each Host country), adapt or develop agreements to support the deployment of visiting police delegations, and make appropriate logistical arrangements (e.g., identify and procure required equipment, accommodation for visiting police delegations, etc.). The deployment of law enforcement officers from other countries, in particular, has been noted as an exemplary form of police cooperation that establishes mutual trust between citizens and their local police and between fans and “their police”.
- Cooperative policing can be further supported by Police Information and Coordination Centres (PICCs). PICCs, which deal with specific event-related security issues, should be set up in each Host country and include liaison officers from participating and neighbouring countries. For example, during EURO 2008, while there were no large-scale exchanges of police between Austria and Switzerland, liaison officers from Austria were posted to host city collaboration centres in Switzerland and vice versa. At the request of a committee of regional police forces, Swiss authorities also requested support from outside the co-hosts’ borders to help manage on-the-ground activities. As

a result, both German and French police forces were deployed to Swiss host cities to support local police.[101]

- Team Security Liaison Officers (TSLOs) have also proven to be a highly effective component of co-hosted events. These Host-country police officers accompany participating teams and serve as links between the teams and the police.

### 3. Create Memorandums of Understanding with participating, transit, and neighbouring countries and with other international organizations

Ministerial-level agreements between Host and other involved countries are recommended to address the following issues:

- sharing of human resources;
- exchange of data related to sport-related incidents and organized crime, terrorism, or other politically-motivated crimes;
- sharing of personal data about high-risk fans;
- preventing potentially violent supporters from travelling to host countries.

All of this should be done in close cooperation with media liaison professionals from local organizing committees and authorities.

Establishing close cooperation with other international agencies (such as INTERPOL, FRONTEX, EUROPOL, RAILPOL, TISPOL) is also important for effective security operations.

### 4. Harmonize security-related legislation between host nations

Coordinating legislation around security-related matters can significantly enhance security operations and improve the overall security of an event. It is recommended that organizing countries harmonize legislation on event-related violence, particularly in relation to criminal penalties and the treatment and extradition of offenders. It is also recommended that Host and competing countries consider legal frameworks for exchanging relevant personal data and measures to prevent high-risk supporters from travelling to an event.

[101] See https://www.dw.com/en/euro-2008-co-hosts-clear-championship-hurdles-mostly/a-3253238 .

-

### 5. Design a harmonized border control framework

Harmonized border-control systems can add value to an event by simplifying international cooperation between security personnel while also enhancing visitors’ experience. For example:

- In preparation for the ICC Cricket World Cup West Indies 2007, the Prime Ministers of the Caribbean Community (CARICOM) designated the nine host venues as “one domestic space” for the duration of the Games, eliminating the need for people to be processed through Customs and Immigration when travelling between these countries. Also, rather than requiring individuals to acquire visas for entering each country, a single CARICOM visa was created for the duration of the event [102]

- Similarly, during EURO 2008, hosted by Switzerland and Austria, a simplified visa process was created to allow individuals to enter both countries with a single visa. However, because Switzerland is not a member of the European Union, border controls were still required. For EURO 2008, a temporary agreement was put in place to establish joint border patrols with personnel from both countries.

- For FIFA World Cup 2026™, the United Bid (Canada, Mexico, and the U.S.) indicated that a task force would be established to address cross-border transport and immigration and international mobility measures through the implementation of a multi-country Fan-ID system once visitors have obtained a visa.[103]

### 6. Harmonize media and communication policies related to security arrangements

Proactive and ongoing communication and media strategies on safety and security measures are a critical component of successful co-hosted events. Policing agencies in organizing countries should work closely with a variety of organizations, including government agencies,

[102] See https://www.espncricinfo.com/story/_/id/22996366/‘historic-caricom-measures-icc-cwc-2007 .

[103] See https://resources.fifa.com/image/upload/2026-fifa-world-cup-bid-evaluation-report.pdf?cloudid=yx76lnat3oingsmnlvzf .

sports organizations, supporter groups, and the media, to prepare and deliver a comprehensive and coordinated strategy. An effective strategy will provide all parties, particularly local communities and event visitors, with important safety and security information, including planned security preparations and measures, travel advice, venue access routes, applicable legislation, and pre-defined behavioural tolerance levels.

### 7. Organize study visits to share practical experiences

Study visits are recommended to provide future organizers with practical insights into security operations. This may be part of the security programme for a regular event (as in the case of UEFA European Championship tournaments) or arranged independently. For example, in 2016, delegates from the Hong Kong Police Force participated in a study visit to the French National Police to discuss counter-terrorism strategies, security planning of major events, policing of public events, and internal security matters. The visit included an experience-sharing session, given by the Director of the Inter-ministerial Delegation for Major Sports Events and the Deputy Head of the Anti-Terrorist Co-ordination Unit, on good practices acquired, and on challenges encountered in hosting international football events.[104]

### 8. Harmonize Public-Private Partnerships with cross-border application

Event organizers should also explore the feasibility of a cross-border application of public-private partnerships when making arrangements for co-hosted an MSE. For example, for the hospitality industry, security functions may often be provided by private companies. Event organizers should keep in mind cross-border challenges in engaging private providers – for example, whether the service provider has in-country presence and relevant licences, whether relevant government stakeholders agree with the engagement of certain private providers. The same considerations should be taken into account for the technological side of security requirements and the challenges to cross-border movement of specific technological equipment. Whilst challenges will prevail in all these areas, with good advanced planning, a harmonized coordination approach towards PPPs should become a seamless process for the smooth delivery of security operations for an MSE.

[104] See https://www.police.gov.hk/offbeat/1074/eng/4597.html .

# X. THE IMPACT OF COVID-19 ON THE SAFETY AND SECURITY OF MSEs

| The economic burden of the COVID-19 pandemic |
|---|
| In the post-pandemic world, the bidding and hosting of MSEs could become more risk-prone, as is already the case with the Tokyo Olympic Games. Originally scheduled for the summer of 2020, the Games have been postponed to July 2021, but might take place in a scaled-down form. At the time of writing (April 2021), many uncertainties remain. The economic, social and medical burden imposed by the COVID-19 pandemic may affect MSE bidding and security requirements for years to come. |

The international community has not seen a public health emergency of the magnitude of the current coronavirus (COVID-19) pandemic since the outbreak of the Spanish influenza at the end of the First World War. The COVID-19 pandemic and consequent lockdowns have imposed severe restrictions on everyone's way of life and present the world, including the world of sports, with unprecedented challenges due to the many uncertainties surrounding the high transmission rate of the coronavirus. At the time of writing (April 2021), it had infected close to 130 million people worldwide and cost the lives of more than 2.7 million persons in 210 countries and territories.[105] While the World Health Organization (WHO), as well as regional and national health and disease control authorities, monitor and try to control the pandemic's course, vaccines were still not universally administered in April 2021.[106]

For those planning MSEs, which generally takes 8 to 13 years or more of preparation, it is tempting to assume that things will have returned to normal once "their" MSE takes place. However, for those Host Authorities who made a successful Bid years ago and where the event is scheduled to take place in the near future – as in the case of the Olympic Summer Games in Japan - the situation is altogether different and a "wait and see" approach is not feasible. Postponing and rescheduling an event brings its own problems and costs with it. Yet even if a rescheduled event actually takes place, the organizers will have to take great precautions and make special arrangements as long as mass vaccination against COVID-19 is notuniversally administered.

[105] As of28 March 2021; see https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases .

[106] https://www.bbc.com/news/world-56237778 .

Guidelines about precautionary measures and arrangements are readily available from the United Nations Department of Economic and Social Affairs[107] and the World Health Organisation.[108] WHO also has a special Unit dedicated to challenges associated with mass gatherings (MGs) and provides support to international sports federations. A selection of guidance currently available from WHO is as below:

- WHO Key planning recommendations for mass gatherings in the context of COVID-19: interim guidance, 2020;[109]
- WHO Considerations for sports federations/sports event organisers when planning mass gatherings in the context of COVID-19, Interim guidance, 2020;[110] and
- WHO Mass Gatherings Sporting Risk Assessment, 2020.[111]

Considerable additional efforts are now required from all MSE organizers to explore and understand the links between organizing MSEs and disaster preparedness and management. More than ever, resilience-building has to be factored in when planning and preparing major sporting events.

The global societal impact of the COVID-19 pandemic highlights the importance for hosting authorities of MSEs to include crises and disaster contingency-planning in their preparations.

[107] Cf. “We Will Help The World Rise Stronger After COVID-19.” UN DESA | United Nations Department Of Economic And Social Affairs; see https://www.un.org/development/desa/en/covid-19.html.

[108] See https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance-publications .

[109] See https://www.who.int/publications-detail/key-planning-recommendations-for-mass-gatherings-in-the-context-of-the-current-covid-19-outbreak .

[110] See https://apps.who.int/iris/bitstream/handle/10665/331764/WHO-2019-nCoV-Mass_Gatherings_Sports-2020.1-eng.pdf .

[111] See https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/points-of-entry-and-mass-gatherings .

# XI. LEGACY CONSIDERATIONS

Security legacy has been defined as “a range of tangible and intangible security strategies, structures and impacts (positive and negative) created for and by a sport mega-event that continue to have significance beyond the life of the event itself”.[112] Beyond this definition, slightly adapting a categorization suggested by Giulianotti and Klauser (2010) for types of security legacy associated with MSEs,[113] this chapter will consider five kinds of security legacies associated with MSEs, namely:

1. Technology and infrastructure
2. International inter-agency cooperation and public-private partnerships
3. Governmental policies and new legislation
4. Social transformations and changes in trans-societal relations
5. Urban regeneration.

## 1. Technology, Infrastructure and Practices

MSEs can be a platform for the development of security technologies in major urban centres, for example, by installing new traffic and other surveillance systems. To this end, as shown in the information box below, MSEs have been become recognized as a ‘laboratories’ for introducing new security systems, such as CCTV networks.

Similarly, an MSE can be an ideal platform to develop a city or country’s security infrastructure. This will be intrinsically linked to the selection of venues, adaptability of existing infrastructure and the political will of decision-makers for using certain parts of a city to deliver an MSE. As such, during the exploratory phase, an assessment of a city’s relevant infrastructure and venues will be an essential step, but always with an eye to the security implications of these decisions.

[112] Preuss, H. (2007b),‘The conceptualisation and measurement of mega sport event legacies’, *Journal of Sport & Tourism*, 12(3-4), pp. 207-228.

[113] Cf. Giulianotti, R. and Klauser, F., “Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda”; see https://www.semanticscholar.org/paper/Security-Governance-and-Sport-Mega-events%3A-Toward-Giulianotti-Klauser/aeaeb821bfbda2a7914082b98679cb0e845a16bc_. The following six categories are suggested by these authors: 1.Technologies; 2. Practices; 3. Governmental policies and new legislation; 4. Externally imposed social transformations; 5. Generalized changes in social and trans-societal relations; 6. Urban redevelopment.

By contrast, in the absence of forward planning and vision, a city may have to build venues and a system from scratch, creating ad-hoc infrastructures that might not last beyond the life cycle of the event itself.

### 2. International and Inter-Agency Cooperation and Public-Private Partnerships

MSEs will inevitably become a platform for enhanced international dialogue, inter-agency cooperation and broader engagement with the private sector. All of these elements have an intrinsic security element to them, and it will be up to the entrepreneurial spirit of public officials and their local partners in the private sector what will become the legacy of an MSE in the field of security.

Security networks established over the course of an MSE may continue to evolve strategic partnerships, knowledge exchange, and expertise, which can be applied to on-going security issues. Similarly, this could lead to new forms of thinking in response to emerging threats and serve as points of consultation for future event hosts. Similarly, proven models and methods to exchange information between public and private-sector operators can generate best practices, which can be applied as lessons learned for the organization of future sporting events.

### 3. Governmental Policies and New Legislation

As explained in Chapter V on Legal and Institutional Frameworks, MSEs often serve as a platform for introducing new policies and legislation, while also providing an opportunity to adopt international standards on certain issues and to adhere to applicable international legal instruments. It could be an opportunity for introducing specific legislation to deal with community policing matters and security (as was the case on the occasion of the 2014 FIFA World Cup™ in Brazil) or to commit the Host country to international human rights standards. It could also lead to new community-related bills, that were long overdue or in the making, as explored elsewhere in this Guide. It could also form a starting point for increased cross-border cooperation of national intelligence agencies.

From a legal standpoint, when it comes to security issues, organizing an MSE can be leveraged to:

- Generate good practices in terms of interagency and international cooperation

- Consolidate legal and institutional frameworks in light of international standards, and a model police and judicial system in terms of protection of human rights.
- Enrich public-private cooperation practices
- Share good practices at national and international levels; and
- Create a platform for better cooperation between government agencies and political parties.

In terms of adopting international norms and adhering to international human rights standards, every MSE is an opportunity to become a good practice model for integrating a human-rights-based approach into the design, implementation, monitoring, and evaluation of security policies and actions as a means to:

- send a powerful message to the international community;
- increase the awareness of citizens to security issues;
- contribute to the overall resilience of the system;
- promote a positive image of sport, the Host Authority, and event sponsors;
- contribute to the prevention of violent extremism by demonstrating a Government's respect for citizens and their human rights; and
- produce legacy impacts that can improve and empower the people of participating nations.[114]

### 4. Social Transformations and Changes in Inter-Community Relations

MSEs are transient, but their effects are often not. MSE security in any specific urban locality also leaves within the host environment a legacy of ideas and practices that can shape the future pursuit of security at the local level. That remains as well as a legacy of "soft event structures", including legislation, and knowledge and practices which may shape the undertaking of safety and security measures at the local level for years to come.

The goodwill generated by including local communities in MSE planning constitutes a form of social capital which can last for a long time.

MSEs can offer an opportunity to empower underprivileged sectors of society and counteract threats like the violent radicalization of vulnerable youth. The jobs, job training, infrastructure

[114] Based on European Commission et al., 2018

improvements, financial investments, and profit-sharing programmes that are often generated as part of an MSE can improve the economic and social outlook of members of disadvantaged communities. More direct activities can also play a role: during the 2010 FIFA World Cup South Africa™, FIFA organized a football competition where local youth could experience the atmosphere of a major sporting event in a safe and fun-filled environment of goodwill and fair play. Moreover, the event engaged the support of other NGOs to offer free HIV tests and other community services. These types of experiences can produce positive, long-lasting outcomes for young people, including for some of those who may be vulnerable to radicalization or criminal influences.

### 5. Urban Regeneration

The organization of an MSE can become the starting point to facilitate urban development or regeneration. Clearing slums, combined with the offering of alternative housing for those affected, can become a lasting legacy for the local community.

**Recommendations:**

**Legacy Considerations**

- → Ensure that the strategies, infrastructure, policies and institutional arrangements specifically put in place for an MSE continue to have significant and produce positive systemic social and economic impacts beyond the event itself.
- → During the planning stage, in particular, consider how the full range of security-related measures and arrangements can be designed and implemented in order to:
  - Consolidate legal and institutional frameworks in light of international standards;
  - Further develop a city or country's infrastructure, including modernising facilities, venues, transport systems and related security components;
  - Consolidate the relationship between governmental agencies and the private sector based on the initial partnership experience created by the MSE;
  - Integrate a human-rights-based approach into the design, implementation, monitoring, and evaluation of security policies;
  - Improve the economic and social outlook of members of disadvantaged communities following, in particular, the employment opportunities generated by the MSE;
  - Facilitate urban development or regeneration.

# XII. GLOSSARY

**Activist Liaison** Police Liaison Officers who proactively discuss protest or demonstration issues with activist leaders. They establish protest guidelines and rules to manage expectations

**After Action Report (AAR)** The document describing the response to an incident and findings relating to performance of the health or security system's response during an incident

**Agency** Any public or private body with constitutional, legislative, regulatory or other responsibility regarding the preparation and implementation of any safety, security or service measure in connection with MSEs, inside or outside of a stadium

**Big Data Networks** The collection, analysis, and use of large amounts of data, from varied and often unstructured, or mostly unregulated, sources

**Bilateral Agreement** Agreement made between two countries, or two organizations that have a functional relationship with the Host Authority

**Biometric Identification** An effective tool for countering the threat posed by a suspect who attempt to travel internationally and use falsified travel documents. Utilizes fingerprints, digital photographs or other biometric capabilities such as AI-based facial recognition.

**Biometrics** Automated means of identifying an individual through the measurement of distinguishing physiological or behavioural traits such as walking style, fingerprints, face, iris, retina or ear features.

**Bioterrorism** The intentional use of micro-organisms, toxins, genetic material or substances derived from living organisms to produce death or disease.

**Border Management** The administration of measures related to authorized movement of persons and goods, whilst also preventing unauthorized movement by detecting those responsible for document fraud, smuggling, trafficking, and related crimes.

**Botnet** The term botnet may be understood to indicate: “a network of computers that have been infected by malicious software (computer virus)”. Such a network of compromised computers (‘zombies’) may be activated to perform specific actions, such as attacking information systems (cyberattacks). These zombies can be controlled - often without the knowledge of the users of the compromised computers - by another computer. This ‘controlling’ computer is also known as the 'command-and-control centre.’” T-CY Guidance Note 2.

**Cabinet Committee** Oversees government policy, spending and legislation and is comprised of Cabinet Ministers responsible for government service delivery to the MSE.

**Capacity** The means that security planners have at their disposal in terms of human, material and technological resources.

**Capacity building** A process that enhances collaboration and competence in sectors or areas of common interest, often by sharing knowledge, skills, equipment, tools and other resources such as technology.

**Change Control Coordinator** Person assessing all aspects of necessary changes in terms of costs, resource requirements, liaising with other planners impacted.

**Command and Control Concept of Operations (C2ConOps)** The integrated and organizational exercise of authority and direction through the proper chain of command over assigned and attached personnel and equipment, within clearly identified areas of responsibilities to accomplish the mission.

**Comply or Explain mechanism** Combines voluntary compliance with corporate governance codes involving a legal obligation (either by law, regulation, or listing rule) to declare compliance with or explain deviations from a code. First used in the U.K.

**Constraints** The quantifiable factors that restrict and regulate the amount or extent of a capacity that can be applied.

**Contingency Plan** Backup plan designed to manage modifications or adjustments to safety and security measures during an ongoing event period so as to respond adequately.

**Controlled Access Zone (CAZ)** The inner perimeter, which includes the stadium seating area and the areas within the stadium overlay where vendors and restaurants may also be found.

**Convention** Formal international agreement between states and/or international organizations.

**Coordinated Border Management (CBM)** Close coordination among the competent authorities at border crossing locations

**COVID-19** A highly contagious disease caused by a coronavirus, transmitted mainly by respiratory droplets but also during contact with objects or contaminated surfaces. Typical symptoms include fever, cough, loss of sense of smell and shortness of breath. More than 137 million people have been affected by early 2021 in 210 countries and territories, with close to 2.7 million deaths (as of April 2021)

**Critical Information Infrastructure (CII)** Interconnected information systems and networks, the disruption or destruction of which would have serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.

**Critical Infrastructure** An asset, system or part thereof which is essential for the maintenance of vital societal functions (esp. related to health, electricity, communication, national security, and financial and economic institutions), the disruption, sabotage or destruction of which has a profound impact on the functioning of government and/or society.

**Crowd Management** Measures taken to assure orderly conduct during mass events, designed to protect spectators, athletes, dignitaries and staff from physical harm.

**Crowded Places** Locations which are easily accessible by large numbers of people on a predictable basis.

**Cyberattack** A malicious attempt by an individual, group or by a clandestine State actor to deliberately breach the information system of a targeted organization or event for sabotage, blackmail, fraud, reputation damage or other purposes.

**Cyber-terrorism** Violent acts committed with the help of computers and the Internet with the purpose of inciting fear, causing harm, and furthering a political, ideological or religious objective.

**Data Protection** Measures designed and/or taken to prevent unauthorized use of private or official information stored or transmitted via computers and the Internet.

**Deliverables** Tangible or intangible goods or services produced as results or outputs of a project intended to be delivered to a customer (e.g. reports, plans, security arrangements).

**Disaster** A natural or man-made occurrence disrupting normal conditions of existence and causing a level of suffering and loss that challenges the capacity of the affected community to cope with it.

**Discrimination** Act of omission or commission making an unjustified distinction, resulting in exclusion or restriction of persons based on grounds such as race, class, colour, ethnicity, sex, language, religion, political opinion, national or social origin, birth or other status. Discrimination leads to impairing or nullifying the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms human beings are entitled to by law.

**Distributed Denial-of-Service (DDoS) Attack** A malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming it or its surrounding infrastructure with a flood of Internet traffic.

**Ebola** A haemorrhagic fever, caused by the Ebola virus and marked by high fever, severe gastrointestinal distress and bleeding. Transmitted mainly by human bodily fluids, it is highly contagious and on average fatal for half of those affected.

**Emergency** A sudden occurrence demanding immediate action or a state in which normal procedures are suspended and extraordinary measures are taken to avert an unwanted situation affecting the health and /or safety of human beings.

**Emergency Management** A range of measures to manage risks to communities and the events caused by extraordinary circumstances.

**Emergency Plan** Group of measures prepared and administered by national or local authorities/organizers for dealing with a major incident occurring at the MSE venue or in its vicinity.

**Event Delivery Authority** Integrated senior government authority responsible for ensuring facilities and infrastructure are built and ready in time for use during event operations period.

**Exploratory Phase (pre-bid)** Phase during which prospective bidders collect cost- and benefit-related information to assist them in their early decision-making as to whether or not to go ahead with submitting a bid.

**Facial Recognition** A camera-based tool for identifying individuals (esp. known troublemakers and criminals) from video-surveillance footage.

**Fusion Centre** Focal point of various stakeholders for the receipt and combination of open-source information and secret intelligence streams to be analysed with an eye to recognizing and countering threats.

**Good Practice** A practice or method of action that has proven to be successful in one situation which can be transferred to similar situations in other contexts.

**Good Governance** Conducting public affairs and managing collective resources in a way that is efficient, accountable and transparent.

**Hooliganism** Disruptive and disorderly behaviour during sport events by groups of usually young and often drunk spectators linked to one or the other competing teams, especially in the context of football.

**Host Authority** The entity or authority responsible for organising an MSE. May refer to the city, region or Government of country or an organizing body. In most cases, the Host Government will refer to a public entity whereas the Host Organizing Committee will be private.

**Host City Guarantees** Commitments made by the host city to the International Sport Federation during the bid phase related to the effective delivery and operation of the event.

**Hosting Agreements** Agreements signed between the International Sport Federation and the Host Authority.

**Information Exchange** The act of individuals, companies and organizations passing information from one to another, especially electronically, or a system that allows them to do this.

**Information Management System** Computer hardware and software system utilized to create, transfer, manage, store and retrieve plans, correspondence, maps, administrative or payroll details, etc., between stakeholders in support of an event and for the historical record.

**Information Sharing** Exchange of information of common interest across organizational boundaries.

**Integrated Approach** High-level planning strategy that, when implemented, brings together multiple planning and execution agencies to prepare for a common outcome.

**Integrated Planning** Structured and standardized framework for preparing a joint outcome based on the input from various stakeholders.

**Interdiction Zone (IZ)** The immediate surroundings of the stadium venue or the outer perimeter where pedestrian and/or vehicle traffic can be observed and stopped when, and if, necessary.

**International Delegations** Groups of persons from other countries visiting an MSE, including participating athletes and support staff (coaches, trainers, administrators), often with special privileges resulting from their official status.

**Interoperability** Situation where instruments of different origin can communicate with each other across technical and other barriers, allowing seamless interactions through synchronization.

**Joint Operational Planning Group (JOPG)** A body of mid-level planners, representing the primary security planning agencies, managed by a Lead Security Agency (LSA).

**Lead SecurityAgency (LSA)** The primary agency that is accountable for the delivery of the event security package. The LSA has oversight over the partner security agencies. Traditionally, the national police service acts as the LSA, ensuring that planning remain focused on the strategic direction, but other bodies can also be designated as LSE.

**Legacy** Valuable and cherished assets or capacities developed and held over as a result of hosting a memorable MSE.

**Lex specialis** Special law governing a specific subject matter. It can override other (older) existing general laws in certain, usually national contexts.

**Local Organizing Committee (LOC)** The officially accredited body responsible for organizing, staging and hosting an MSE.

**Multilateral Agreement** Agreements between three or more States on economic, legal, military or other matters.

**Multi-sectoral** Involving multiple sectors; also referring to an approach in which a problem is addressed from various angles.

**Operational Command Structure** Structure outlining the command authority for safety and security operations during an MSE, including normal operations, incident command and transfer of authority protocols.

**Operational Plan** Plan for the delivery of operations, by individual units or collectively, during the event. It includes Standard Operating Procedures (SOPs) for regular activities.

**Options Analysis** The practice of evaluating during a planning phase every possible pathway that could lead to a desired outcome.

**Organizational Interdependencies** Situations where the actions (or non-actions) of one-unit impacts (negatively) on the functioning of one or more other units which together produce a joint product such as an MSE.

**Planning Component** Part of a planning structure with its own character that needs to be harmoniously integrated into the larger framework to ensure a successful outcome.

**Preparedness** Taking pro-active and pre-emptive measures, based on planning and practising (training) of voluntary or professional units to reduce risks and threats and, if that turns out to be insufficient, reduce the negative impact of unwanted occurrences through a set of precautionary measures aimed at strengthening readiness and resilience.

**Prevention** The taking of measures to remove the causes of an undesirable development or to obstruct the occurrence of an unwanted situation; social and technical engineering to reduce individual or collective harm or damage by inhibiting, dissuading or deterring potential malevolent actors and also by creating environments where harmful activity is made more difficult.

**Private Security** Licensed commercial enterprise performing certain public-order maintenance functions with trained personnel, usually unarmed and without the power to arrest, hired to fulfil specific duties at MSEs, under the supervisory oversight of the official police forces.

**Protection** Activities aimed at ensuring the well-being, functioning and integrity of human beings and facilities, including critical infrastructure, to deter, mitigate and neutralize threats to life and limb and to uphold law and order.

**Public Health Security** Activities required, both proactive and reactive, to minimize vulnerability of individuals and groups of people to known health hazards endangering their well-being.

**Responsibility and Accountability Matrix (RAM)** A project management tool that assigns obligations to various parties/partners in an organization and holds these responsible for completing tasks or present deliverables for the project's overall progress.

**Restricted Access Zone (RAZ)** Areas with the most limited public access such as the Field of Play where only athletes/players and certain field maintenance crews, television/media, game and field officials, referees, doctors, first aid teams, players, and security have access.

**Risk Assessment** Process used to determine level of risk in a given situation, present or future, by evaluating and comparing given level of risk to pre-determined standards, target risk levels, or other criteria.

**Risk Management** A systematic approach to identifying, addressing and reducing risks of all kinds associated with natural hazards and human activities.

**Rule of Law** Mechanism, process, institution, practice or norm that supports the equality of all citizens before the law, secures a non-arbitrary form of government, and more generally prevents the arbitrary use of power.

**Safety** Condition of being protected from harm or undesirable outcomes, including health hazards or attacks on a person’s physical integrity. It also can refer to a normal, low-risk or acceptable risk situation.

**Security** In the context of an MSE, the concept of security incorporates all measures designed to deter, prevent, and sanction any incident of violence or harmful misbehaviour inside or outside of a stadium.

**Security Measures** All measures designed to deter, prevent, and sanction any incident of violence, or harmful misbehavior committed in connection with a sports event, inside or outside of a stadium.

**Security Operation** Action carried out by lawful authorities, such as arrest of a dangerous person or criminal offender, search and seizure of arms that someone may carry, and investigation of the incident.

**Security Planning** Activity that involves designing, implementing, monitoring, reviewing and improving practices for creating a safe and secure environment for a planned event.

**Senior Executive Team (SET)** The heads of the key event stakeholders from the Government and the Host organizing committee.

**Service** The concept of service comprises all measures designed to make MSEs enjoyable and welcoming for all, in stadiums but also in public spaces where spectators and supporters gather before, during and after the event.

**Service Measures** All measures designed to make events enjoyable and welcoming for all.

**Soft Targets** Places and venues that are easily accessible to large numbers of people and that have only limited security or protective measures in place, making them vulnerable to attack.

**Sports diplomacy** The deliberate, strategic use of sporting events by Governments to create a favourable international image for their country - the "continuation of politics by other means," whereby sports, nationalism, diplomacy as well as commerce become inextricably linked.

**Spotters** People who support policing operations by gathering relevant information and intelligence on spectators and supporter groups in real time.

**Stakeholder** Spectators, local communities or other interested parties who do not have legislative or regulatory responsibilities but who can play an important role in helping to make MSEs safe, secure and welcoming, inside and outside of stadiums.

**Standard Operating Procedures (SOPs)** Detailed, written instructions on how employees are to perform routine tasks and activities.

**Stewards** Private security and service providers employed by the event management. They assist spectators, respond to any complaints, react to incidents and emergencies and help the police and emergency services as required

**System Inputs** Contributions which, when brought together in a planned and organised way, form a strategic combination capable of achieving desired objectives.

**Systems Building** Systems Building involves three primary elements. These are comprised of sub-systems that are systems in and of themselves; are made up of processes or activities that interact and/or are interdependent; and are established for the purpose of meeting specific goals and objectives. Systems are comprised of inputs, processes and outputs.

**Target Audience** Group of persons for which activity is prepared. It can, in the case of an MSE, and depending on purpose, consist of policy makers, decision makers and chief planners from Ministries of Interior/Security/Public Order/Sport, international, continental and national sport federations, bidding committees, or local organizing committees.

**The Cabinet Committee** Senior-level Government committee made up of Ministers responsible for resources, authorizations and services related to the event.

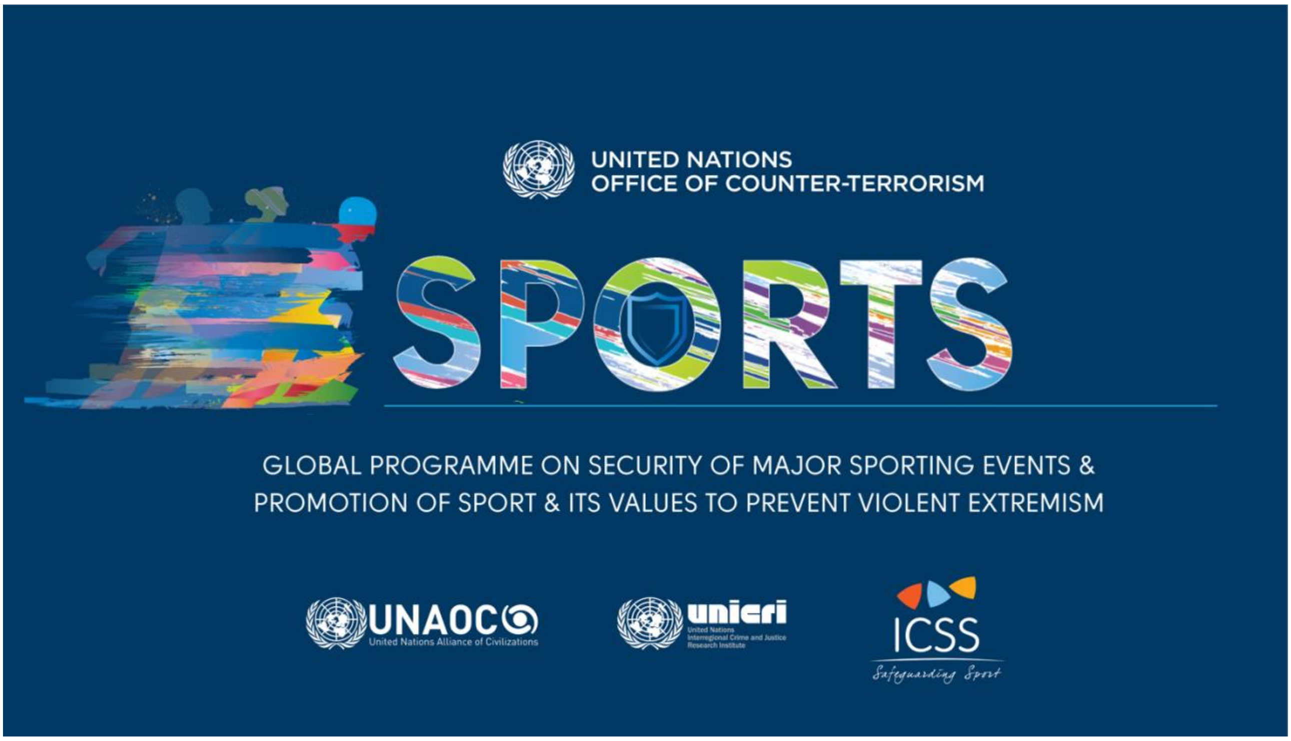
**Treaty** A legally binding international agreement concluded between States or international organizations governed by international law, whether embodied in a single instrument or in two or more related legal instruments.

**Unified Command Centre** In the context of an MSE, the operational command centre which incorporates all the main safety and security service providers, including key public and private-sector security stakeholders.

**Vehicle (VSA) and pedestrian (PSA) screening** Process of visual or physical control conducted prior to any vehicles (service, team or official) or pedestrians entering a Controlled Access Zone

**Visiting Police** Uniformed police forces from other countries other than the one organizing an MSE, invited to accompany athletes, players, official functionaries or VIPs.

UNITED NATIONS OFFICE OF COUNTER-TERRORISM   unicri United Nations Interregional Crime and Justice Research Institute   UNAOC United Nations Alliance of Civilizations   ICSS Safeguarding Sport


UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
SPORTS
GLOBAL PROGRAMME ON SECURITY OF MAJOR SPORTING EVENTS &
PROMOTION OF SPORT & ITS VALUES TO PREVENT VIOLENT EXTREMISM
UNAOC United Nations Alliance of Civilizations
unicri United Nations Interregional Crime and Justice Research Institute
ICSS Safeguarding Sport

# UN Guide on the Security of Major Sporting Events

## XIII. ANNEX

Examples of country approaches

## • Argentina

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Buenos Aires Integrated Regime for Football Events

As in other countries over the past few decades, Argentina has suffered from major problems with football hooliganism. Eighteen (18) major stadiums regularly host MSEs and fan violence and hooliganism are a constant threat. To mitigate this threat, the country has passed several laws and regulations that evolved from the criminalization of specific conduct to the establishment of a comprehensive regime, a decision which had a positive impact with the creation of an updated framework to protect sporting events of international relevance.

In 2017, the Government approved the Integrated Regime for Football Events of the Autonomous City of Buenos Aires.[141] The new law focuses on security aspects, such as the physical integrity of spectators and participants, and countermeasures to mitigate hooliganism and fan violence. Provisions aimed at preserving a pleasant atmosphere to make events enjoyable and welcoming, in line with the service aspects enshrined in the Saint-Denis Convention, however, are not addressed in the Integrated Regime. The 2017 Integrated Regime was built upon the Integral Security System of the Autonomous City of Buenos Aires, established in 2016.

During the organization of the Youth Olympic Games (YOG, Buenos Aires, 2018), the Buenos Aires Ministry of Security issued Resolution 179/ISSP/18 on Private Security for this MSE.[115] This resolution approved the establishment of a working group aimed at developing capacity, measures and policies to enhance key security aspects during the YOG. In particular, the working group based its work on the Integrated Regime for Football Events and the Integral Security System of the Autonomous City of Buenos Aires.

## • Australia

## THE SECURITY PLANNING SYSTEM

### Categories of Plans

Example – Australia's Strategy for Protecting Crowded Places from Terrorism, 2017

The essentials of a robust plan for protecting sites and public places from terrorism should consist of:

- building strong, sustainable partnerships between Governments and the private sector;
- enabling better information sharing;
- implementing effective protective physical security measures; and
- increasing resilience.[116]

## LEGACY CONSIDERATIONS

One of the most important legacies consists of lessons learned from previous MSEs. For example, in an interview with a representative of the FIFA Women's World Cup™, it was acknowledged that the Australian bid for the 2023 World Cup was presented in a very persuasive way as regards security issues. It was in part because of having hosted the Asian Cup in 2015, that Australia and New Zealand won the right to hold the 2023event.

[115] See https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-ISSP-179-18-5464.pdf .

[116] Australia-New Zealand Counter-Terrorism Committee. "Australia's Strategy For Protecting Crowded Places From Terrorism." Australian National Security, 2017; see https://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/australias-strategy-for-protecting-crowded-places-from-terrorism.aspx.

- **Brazil**

## FOUNDATIONS OF SECURITY AT MAJOR SPORTING EVENTS

### Proper Estimate of Security Costs

While to some extent a law adopted explicitly for a specific MSE or for dealing with sport security in general may derogate from existing laws and regulations (as a Lex specialis), its role is first and foremost to act as a coordinating tool, ensuring the smooth application of legal and institutional powers already present under existing national laws. For example, host nations may want to avoid situations where the preparation of an MSE could be jeopardized by fragmented or overlapping regulations. This may, for instance, be the case where difficulties are expected in determining which authority should be responsible for health services in the zone outside the stadium premises. This might create organizational friction that could be avoided by enacting an overarching law for an MSE.

For instance, the Brazilian Law on the FIFA 2013 Confederation Cup and the 2014 FIFA World Cup™ [117] established a special regime to coordinate all security and organizational matters. Likewise, in preparation for the Olympic Games in Brazil, the Government adopted the Strategy for Rio 2016[118], aimed at guaranteeing security in a discreet and fan-friendly way. The strategy addressed all the services related to public security, national defence and intelligence that were deemed necessary to guarantee a safe and peaceful environment for the local people, visitors and participants in the Games, ensuring that there would be no inconsistencies in the organization and implementation of the MSE.

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Specific MSEs Strategies and Laws to Strengthen the Existing Legal Framework

In 2014 and 2016, Brazil held two MSEs, the FIFA World Cup™ and the Summer Olympic and Paralympic Games. 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 organisation and implementations of both MSEs. To this end, Brazil enacted specific laws attributing responsibilities, and enabling law enforcement and military forces to effectively operate within the particular context of an MSE.

In 2014, the Ministry of Defense approved Document MD33-M-10 “Garantia da Lei e da Ordem”,[119] which defined the scope of action of military forces. This policy document includes several of the international standards described above, such as coordination and cooperation measures, exchange of information, and integrated approaches to share intelligence and effective communication.

The Government also passed a Law concerning the FIFA 2013 Confederation Cup™ and the 2014 FIFA World Cup™,[120] establishing a special regime during the hosting of those MSEs. In terms of security within the stadium and in contiguous zones, the law refers to the Federal Police Statute for Private Security Agencies,[121] which governs all aspects related to private security. For the Olympic Games, the Government adopted the Strategy for Rio 2016.[122] The strategy addressed all the services related to public security, national defence and intelligence necessary to guarantee a safe and peaceful environment for visitors and participants of the Games.

### Example – Proteja Brasil

[117] See https://presrepublica.jusbrasil.com.br/legislacao/1032211/lei-12663-12

[118] See http://www.rededoesporte.gov.br/es/presskit/archivos/fact-sheet-seguridad

[119] See https://www.gov.br/defesa/pt-br/arquivos/2014/mes02/md33a_ma_10a_gloa_2eda_2014.pdf/view

[120] See https://presrepublica.jusbrasil.com.br/legislacao/1032211/lei-12663-12

[121] See http://www.pf.gov.br/servicos-pf/seguranca-privada/servicos/autorizacao-de-funcionamento-de-empresa

[122] See http://www.rededoesporte.gov.br/es/presskit/archivos/fact-sheet-seguridad .

Proteja Brasil is an app developed for tablets and smartphones to facilitate the identification and notification of child rights violations within the context of a major sporting event. It was launched in 2013 and widely promoted at the 2014 FIFA World Cup Brazil™ and the Rio 2016 Olympics in campaigns to protect children and adolescents from physical violence, child labour, sexual exploitation, neglect, and discrimination.

Source: "Proteja Brazil." Save The Dream, http://savethedream.org/2019/06/30/proteja-brazil/

- **Canada**

## FOUNDATIONS FOR SECURITY AT MAJOR SPORTING EVENTS

### Leadership and Vision

Values that the organization feels are important to fulfil should be set at an early stage. The organizational core values should become part of the mission statement of the whole event and form part of the blueprint from which all organizational groups, including security, can align their strategies in accordance with their respective mandates. The security mission of the MSE, should, therefore, be incorporated into the broad vision of the MSE and aligned to the organizational core values.

For example, the mission statement from the Security Functional Area (FA) for the 2015 Pan American Games was: "Provide a safe and secure environment for the conduct of the 2015 Pan Am/Parapan Am Games while maintaining an open, accessible and authentic experience for athletes and attendees; aiming to minimise disruptions to residents, businesses and visitors". Similarly, the mission statement related to the transportation function for the Pan American Games was, "All accredited athletes and officials will be provided with safe, secure and reliable transportation services that ensure timely delivery to and from all accommodations and Games venues". [123]

## THE SECURITY PLANNING SYSTEM

### Private Security Services for the Vancouver 2010 Olympic and Paralympic Winter Games

It has become a common occurrence to see private security personnel perform certain duties at MSEs around the world, under the supervision of the major event's lead police agency. The use of private security, complementing the functions of the lead police agency and their police and military security partners, has proven successful. It allows official security forces to focus on their core security mandates and provides more efficient security coverage during an event.[124] Private security officers, as well as the Stewards and Security Volunteers, become "force multipliers" in support of the MSE Safety and Security mandate.

### Example – Private Security within the Olympic and Paralympic Games and the Pan Am and Parapan Games

Within MSEs such as the Olympic and Paralympic Games and the Pan Am and Parapan Games, Private Security has been used successfully for tasks including:

- Ticket and accreditation validation (spectator and visitor control systems);
- Access control to venues and Athletes' villages;
- Hospitality events access systems;
- Pedestrian Screening Area (PSA) screening functions (baggage, handbags, and backpacks' checks search equipment, body wand);
- Badge issuance and control;
- Patrol the designated premises or area; and

[123] Let's GO! Toronto 2015 Pan Am / Parapan Am Games Strategic Framework for Transportation Version 4.2 – February 2014, Volume 1, pg. 3, Queen's Printer for Ontario; see http://www.mto.gov.on.ca/english/panam-games/pdfs/strategic-framework-for-transportation-volume-1-en.pdf .

[124] Addressing the role of private security companies within security sector reform programmes; see https://www.files.ethz.ch/isn/39540/PSC_report.pdf .

- Monitor and respond to intrusion and safety alarms. [125]

**Example – Private Security Services for the Vancouver 2010 Olympic and Paralympic Winter Games**[126]

The private security service provider was contracted to deliver multiple Games services to the 2010 Winter Games. The contractor worked in a public-private partnership with the Royal Canadian Mounted Police Integrated Security Unit (ISU), Public Works, Government Services Canada (PWGSC) and the Vancouver Organizing Committee (VANOC). The contractor delivered the full private security services for the Olympic Event Services Program, the Asset Protection Program and the Games Security Screening Services. The total scope included more than 35 venues, 400 management personnel, and 12,000 Games-time staff.

Private security contract: quick facts

- ✓ 350 days of operations at 26 venues (24/7)
- ✓ Coordinated schedules for 100,000-plus shifts
- ✓ About 60,000 trips (transport)/ 2,150 on peak days
- ✓ More than 72,000 individual uniform pieces distributed
- ✓ 5,200 staff deployed on peak days
- ✓ 2 million people screened
- ✓ Delivered training for 16 hours daily, seven days per week for five months
- ✓ 7,500 resumes received, hiring more than 300 full-time managers
- ✓ 20,000 other applications reviewed
- ✓ 60,000 bed nights
- ✓ 1,000 radios
- ✓ 180,000 meals
- ✓ Contract duration: 11.5 months.

Games time staff recruitment

- ✓ Hiring start: 25 July 2009
- ✓ French – 628 fluent speakers
- ✓ Out of State – 1,150 hires
- ✓ 6,000th hire: 17 November 2009
- ✓ First Nations – 550 staff
- ✓ Average age: 36.6 (female) and 37.4 (male).

Successes

- Positive working relationship with ISU/PWGSC/VANOC (Note: all parties shared common goals)
- No major security incidents - Vancouver 2010 resulted in the largest private security workforce in Canada at the tine
- A successful model of integrated operational planning and reporting
- Aligned communication and public relations strategies; and
- Successful recruitment, training, development and support programs

## COMMUNICATION STRATEGIES

### Community Relations Group

The Community Relations Group (CRG) should build a relationship of trust, mutual understanding and respect between the ISCT and all stakeholders/external parties. The CRG should actively engage affected community members to educate and keep them appraised of the MSE and its likely impacts. A Community Activist Liaison (CAL) component should be established to ensure that there is a dialogue that acknowledges activists' rights to protest. They should be advised of police expectations, actions and consequences. CALs can be used to help enforce designated protest areas.

[125] Guidelines on the Use of Armed Security Services from Private Security Companies, see https://www.ohchr.org/Documents/Issues/Mercenaries/WG/StudyPMSC/GuidelinesOnUseOfArmedSecurityServices.pdf .

[126] Information provided by Stephen V. Mirabile, President and CEO, CSC Canada.

**Example – 2010 Vancouver Winter Olympics "Spirit Train" blocked by Activists**

In 2010, activists blocked the Olympic "Spirit Train" a.k.a. the Cheesy Choo Choo, as it approached Toronto, by blocking the tracks and occupying a railway bridge. This highly coordinated and well-executed non-violent action was taken in solidarity with the Olympic Resistance Network of British Columbia, the Native Youth Movement of the Coast Salish People, and the Anti-Poverty Committee of Vancouver, who had called for actions against the Spirit Train and all 2010 Olympic Games-related activities. The situation was tense at times, but the Activist Liaison negotiated with the police, and after a three-and-a-half-hour blockade, a peaceful de-escalation resulted, and no one was arrested. [127]

.

- **France**

## V. LEGAL AND INSTITUTIONAL FRAMEWORKS

### Strengthening national legal and institutional frameworks to secure MSEs

It is of paramount importance that Host nations be not only "operationally", but also "legally and institutionally", prepared. There are two methods that Host nations can follow to adapt their legal and institutional frameworks to the multiple requirements that the planning, organization and implementation of an MSE require:

- Countries may introduce and/or amend existing pieces of legislation dealing with the various aspects of security relevant for the planning and conduct of an MSE; or
- Countries may enact an overarching law specifically addressing a forthcoming MSE or sport security.

An example of the former is the 2018 French law for the organization of the 2024 Olympic Games,[128] as this law was enacted to specifically tackle this particular event. An example of the latter is the 2009 Colombian law on the security of sports events. Broad and generic, it seeks to govern all sports events organized in the country.[129]

**Law for the Paris 2024 Olympic Games**The French Law for the Paris 2024 Olympics[130] was enacted on 26 March 2018, six years before the opening of the Games. The law covers all aspects relevant to the security of the MSE, following international standards and delineating the authorities in charge of each matter. It includes provisions that temporarily revoke the validity of specific regulations during the implementation of the MSE. For instance, specific provisions of the urban planning code will be suspended (Art. 10). The law further establishes that it will be complemented by subsequent decrees, e.g., creation of an interagency coordinating commission. It is heavily informed by the the Vigipirate Plan[131] , the national strategy on countering terrorism, which had been upgraded in response to the 2015 and 2016 major terrorist attacks in France.

## THE SECURITY PLANNING SYSTEM

### The Vigipirate Plan

The Vigipirate Plan is a central tool of the French anti-terrorism strategy. It lists 300 measures that apply to 13 action areas, such as facilities, buildings and mass gatherings. The Plan rests on three pillars (vigilance, prevention and protection) and involves all actors, including the State, local authorities, businesses and citizens. Since 2015, France has prioritized the protection of soft targets, including places of worship and sports venues.

## COMMUNICATION STRATEGIES

[127] "Departure Of Olympic 'Spirit Train' Met With Protesters In B.C." Thestar.Com, see https://www.thestar.com/news/canada/2008/09/21/departure_of_olympic_spirit_train_met_with_protesters_in_bc.html

[128] See https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036742943?r=2Xd1Gp7YbJ .

[129] See https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=37645 .

[130] See https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036742943?r=55PGTjBBGC .

[131] See https://www.gouvernement.fr/vigipirate .

**The Social Charter for Responsible Games**

**Example - 2024 Paris Olympic Games**

For the 2024 Paris Olympic Games, The Social Charter for Responsible Games was signed by trade unions and employers groups together with the city of Paris and the COJO (Organizing Committee of the Olympic Games) to protect workers and ensure that social and economic development with medium to long-term results becomes an integral part of the legacy of the 2024 Games. This is followed by the Government's intention to regenerate the Saint-Denis area and to provide opportunities for people residing in the *banlieue* (outskirts of Paris). [132]

## LEGACY CONSIDERATIONS

### Technology, infrastructure and practices

MSEs can be a platform for the development of security technologies in major urban centres and have been become recognized as "laboratories" for introducing new security systems, such as CCTV networks.

At its best, an MSE can be a platform for modernizing facilities, venues, transport systems and related security components. For example, the infrastructure built for the organization of the 1998 FIFA World Cup France™ was used to organize the 2007 Rugby World Cup, the UEFA Euro 2016, and the FIFA Women's World Cup 2019™. Similarly, organizers for the FIFA World Cup Qatar 2022™ intend to construct a number of modular stadiums that can be shipped overseas after the World Cup in order to be re-utilized in new locations. In most cases, integrated security elements could be transferred to the new environment.

- **Germany**

## STAKEHOLDER COOPERATION

**Security risk management strategy, bilateral agreements**

Information-sharing mechanisms for MSE security are often built upon existing relationships with other countries. In their absence, these mechanisms should be built into existing infrastructures for international intelligence exchange. For example, for each Olympic Games event since Atlanta 1996, organizers have created an Olympic Intelligence Centre (OIC) to assemble information and risk assessments based on cooperation and information-sharing protocols involving over a hundred countries and international organizations. The support of international policing agencies is critical with respect to intelligence sharing.

**Example – The 2006 FIFA World Cup Germany™**

For the 2006 FIFA World Cup Germany™, the country developed its security risk-management strategy around bilateral agreements with 36 other countries that had been employed in previous European tournaments and the Athens 2004 Olympic Games, building upon ongoing and existing information flows that focused on hooliganism. Germany also signed bilateral agreements with all participating countries and several neighbouring and transit States to control and restrict border crossing of "undesirable" fans to reduce incidents of hooliganism.[133]

[132] Charte Sociale des Jeux Olympiques et Paralympiques, Paris 2024; see https://www.paris2024.org/app/uploads/2019/10/DP_Jeux-de-2024-Des-opportunites-pour-tous_VF71.pdf

[133] Aas, Katja Franko. *Technologies of In Security*. Routledge, 2008.

- **Greece**

## STAKEHOLDER COOPERATION

**Athens 2004 Summer Olympics Security Networks: Resource Sharing**

The secondment of police officers to support the Host country's forces provides not only a greater law enforcement presence and capacity but also resonates with fans when "their own" police are present at an event. These types of secondments may also extend to emergency response, health, and other relevant security-related sectors. Host Authorities may also benefit from borrowed equipment or technology-based platforms from international partners. However, not every stakeholder will have equal levels of capacity or resources to contribute. A capacity assessment, with input and analysis provided by multi-disciplinary subject matter experts, is recommended to determine the capabilities of each partner and to provide a road map for building the necessary security capacity (see Chapter VII on the Security Planning).

**Example – Athens 2004 Summer Olympics Security Networks**

A prime example of capacity assessment, with input and analysis provided by multi-disciplinary subject matter experts, was demonstrated during preparations for the Athens 2004 Summer Olympics. At the time, seven countries - Australia, France, Germany, Israel, Spain, the United Kingdom, and the United States - formed the Olympic Security Advisory Group (OSAG). This group provided coordinated security advice to Greece, provided training, donated equipment, and worked in a cohesive and transparent manner to address specific vulnerabilities and ensure Greece received the best possible support. [134]

**Counter-Intelligence Security Unit**

Example – Greece's reforms of security organization for the future

The Athens 2004 Olympic Games was the first Olympics hosted post-9/11, the terrorist attack which greatly changed the security context of MSEs. The Greek Intelligence Service (NIS-EYP) was reformed, and the Government established:

- A Study Center to enable collaboration between scientific organizations, universities and specialized research institutes. It examined and analysed topics of interest to the NIS-EYP;
- A strategic Staff Planning Council (steering committee) to deal with crisis management and implement policies;
- A Training Directorate to modernize staff training;
- A Sub-Directorate for National Issues;
- A Directorate for International Cooperation, for improved exchange of information with allied services; and
- A Sub-Directorate for International Terrorism and Organised Crime for the NIS-EYP.

The Counter-Intelligence Security Unit was elevated to a Directorate to deal with new security issues.

## LEGACY CONSIDERATIONS

**Social Transformations and Changes in Inter-Community Relations**

MSEs are transient, but their effects are not. MSE security in any specific urban locality also leaves within the Host environment a legacy of ideas and practices that can shape the future pursuit of security at the local level, as well as a legacy of "soft event" structures, including legislation, knowledge and practices which may shape the undertaking of safety and security measures at the local level for years to come.

**Example – Athens 2004 Olympic and Paralympic Games**

[134] Ibid.

Athens benefitted from improved infrastructure as a result of hosting the 2004 Olympic and Paralympic Games, including:

- The opening of the Eleftherios Venizelos International Airport (which welcomed 25,500,000 passengers in 2019)
- 90 km of new roads and another 120 km of improved roads
- A new computerized traffic-management system
- A new and renovated underground system which currently transports one million passengers daily (20 per cent of the city's population)
- Partially as a result of the Olympics, the number of tourists increased in subsequent years.[135]

- **Japan**

## STAKEHOLDER COOPERATION

### International Cooperation

While security-related concerns cover a broad field of stakeholders, the main aspects to consider can be classified into bilateral and multilateral agreements, threat-risk assessments, information-sharing, resource-sharing, capacity-building and technical assistance, spotters and security networks.

### Capacity-building to enhance security at the 18th Asian Games and at the 30th Southeast Asian Games

In 2018, Japan provided a facial-recognition system and a behaviour detection system to Indonesia, the host of the 18th Asian Games, through official development assistance (ODA). Additionally, Japan provided capacity-building assistance by organizing the "ASEAN-Japan Workshop to Promote the Use of Biometric Technologies for Enhanced Security", aimed at enhancing the capacities of airport security officers in ASEAN Member States by utilizing the systems provided to Indonesia.

In 2019, as part of INTERPOL's "Project Riptide", funded by the Government of Japan and aimed at tackling foreign terrorist fighter (FTF) movements in Southeast Asia, the INTERPOL Major Events Support Team (IMEST) was deployed to the 30th Southeast Asian Games, resulting in the arrests of more than 25 internationally wanted persons.[136]

### Public-private partnerships (PPP):

### Overseas Security Advisory Council (OSAC) and the Tokyo 2020 Olympics

- Cooperation between sponsors and other corporate stakeholders can be optimized in many ways. It is recommended that a Host country involve them early in the planning dialogue as this may reveal new perspectives, information, or approaches that can be employed as part of the wider security plan. For example, the security cultures, procedures, and risk assessment/mitigation models applied by global corporations might provide important insights for security planners. Including sponsors in early capacity assessments can also prove valuable for enhancing and coordinating security resources. Establishing public-private associations could also promote knowledge-sharing and best practices, based on prior or specialized experience.

### OSAC and the Tokyo 2020 Olympics

During the exploratory phase, the Overseas Security Advisory Council of the US Department of State organized in-person discussions between sponsor organizations and government officials as part of their inclusive and well-organized collaboration model.

[135] "Athens Infrastructure Boosted by Olympic Games 2004." International Olympic Committee, 19 Jan. 2016; see https://www.olympic.org/news/athens-infrastructure-boosted-by-olympic-games-2004.

[136] Source: Permanent Mission of Japan to the United Nations.

- **People's Republic of China**

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Experience and Practices for the Security of Major Sports Events

Chinese legislation defines an MSE as any sports event organized by an entity or their juridical person, which is open to the general public and in which the anticipated attendees exceed 1,000 per event. The Government of China prioritized security in MSEs by incorporating counter-terrorism measures into its national security strategy. Based on the scale of the sports event, a national-level security liaison has been established to enhance the capacity of terrorism-related intelligence information collection, the security of high-profile individuals, venue security and identification check, street patrol, traffic control and MSE safety activities.

Other relevant Chinese legislation included in the Criminal Code foresees the punishment for disorderly conduct such as hooliganism. In addition, in order to strengthen the security of large-scale mass activities such as sports events, and protect citizens' lives and property and to maintain public order and safety, the Government of China issued and implemented the "Regulations on the Safety Management of Large-scale Mass Activities". The regulations establish a chain of command in public security, improve safety management measures, regulate the behaviour of participants, and stipulate legal consequences for violations. The aforementioned laws and regulations established a legal framework and provided a concrete legal basis for the security and for counter-terrorism activities during MSEs held in the People's Republic of China.

## CO-HOSTING MAJOR SPORTING EVENTS

### Organize study visits to share practical experiences

Study visits are recommended to provide future organizers with practical insights into security operations. This may be part of the security programme for a regular event (as in the case of UEFA European Championship tournaments) or arranged independently. For example, in 2016 delegates from the Hong Kong Police Force participated in a study visit with the French National Police to discuss counter-terrorism strategies, security planning of major events, policing of public events, and internal security matters. The visit included an experience-sharing session given by the Director of the Inter-ministerial Delegation for Major Sports Events and the Deputy Head of the Anti-Terrorist Co-ordination Unit on good practices acquired and challenges encountered in hosting international football events.[137]

- **Republic of Korea**

## POLITICAL, ECONOMIC AND SOCIAL DIMENSIONS OF MAJOR SPORTING EVENTS

MSEs are major undertakings for Host Authorities and the motivations underlying the organization of a sporting event of such international magnitude usually exceeds the world of sports.

Despite the objective difficulty in accurately evaluating the real economic costs of hosting an MSE, and regardless of the fact that in recent years many citizens have come to look at MSEs with an increasingly skeptical eye, it is undeniable that MSEs have repeatedly obtained international, and at times even geopolitical relevance. MSEs also offer opportunities to promote positive change within a Host country as well as for the international community at large. MSEs have social, political and diplomatic dimensions, offering an opportunity to strengthen international dialogue.

The history of MSEs also show how Host Authorities have used the organization of a major sporting event to bring about positive change and reduce political tensions, as in the case of the 2018 Winter

[137] See https://www.police.gov.hk/offbeat/1074/eng/4597.html .

Olympics in Pyeongchang, which brought the Democratic People's Republic of Korea and the Republic of Korea closer together.

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Guidelines for Security of MSEs and Counterterrorism

The National Assembly of the Republic of Korea enacted the International Athletic Game Support Act,[138] followed by provisions for administrative and financial cooperation between national and local Governments. Under the Act, an organizing committee may be established to prepare and host an athletics competition along with financial assistance from national or local governments.

For the Pyeongchang 2018 Winter Olympics and Paralympics, special laws and enforcement ordinances were introduced to establish counter-terrorism measures tailored to the Winter Olympics. In order to implement these measures effectively, the National Counter-Terrorism Center (NCTC) and the National Intelligence Service (NIS) jointly formed the headquarters for counter-terrorism countermeasures, pursuant to the Act on Counter-Terrorism for the Protection of Citizens and Public Security (the "Anti-Terrorism Act"), in close liaison with the organizing committee, the IOC, and other bodies from relevant countries.

As for other MSEs in Korea, the Government established an organizing committee based on the international competition support law and installed a Terrorism Safety Response Headquarters with the NCTC and NIS.

## • MERCOSUR

For many MSE security experts, the multilateral approach is preferred. It is also essential for ensuring that smaller or less experienced countries can benefit from the knowledge, advice, and resources of more experienced or affluent countries in the development of security frameworks. However, multilateral cooperation usually takes ~~a~~ more time and effort to negotiate than bilateral agreements due to their greater complexity.[139]

### Example – Multilateral Agreements: Guidelines on Security Matters in international football events in MERCOSUR State Parties and Associated States

On 7 June, 2012 MERCOSUR (Southern Common Market) State Parties signed a multilateral agreement aimed at promoting the establishment of public policy guidelines for~~t~~ the prevention of violence at international football events between national teams or sports institutions of their Member States. The multilateral agreement also aimed at formalizing a network of contacts between the main actors and institutions involved in the development of international football matches that allow coordinating actions aimed at optimizing security before, during and after the international football event. It also defined the type of information to be exchanged and promoted mechanisms for the exchange of this information that are appropriate to national and international standards, especially those referring to the protection of personal data.[140]

[138] Act No. 15812, Oct. 16, 2018.

[139] Adhikari, S. (2019, December 23). 10+ Differences between Bilateral and Multilateral Cooperation. *Public Health Notes*; see https://www.publichealthnotes.com/10-differences-between-bilateral-and-multilateral-cooperation .

[140] Source: Ministry of the Interior and Public Security of Chile.

- **The Philippines**

## THE SECURITY PLANNING SYSTEM

**2019 Southeast Asian (SEA) Games in the Philippines**

A layered approach should be considered for the protection of MSE venues.

**Example – 2019 Southeast Asian Games in the Philippines**

During the 2019 SEA Games, the Senior Task Force collaborated with the Games Organizing Committee on security arrangements for five zones:

- The Public Zone included the city,  areas outside of the venue district and transportation hubs
- The Exclusive Zone included the area of commercial activities specifically linked to the event
- The Outer Zone included the outer edge of the venue where police and security conducted security checks and access control operations. Emergency staging areas were identified near the venue within the Outer Zone.
- The Inner Zone included the line of demarcation between the outside and the inside of the venue. Only people with valid tickets and proper credentials could pass the demarcation into the venue which included secure and areas of shelter for spectators.

- **Poland**

## CO-HOSTING MAJOR SPORTING EVENTS

**Set up joint preparations well in advance, including the establishment of agreements between Governments and relevant multinational working groups**

In 2008 the Government of Poland and the Cabinet of Ministers of Ukraine signed an agreement for cooperation for the organization of EURO 2012, including the planning of safety and security. In 2010, a Polish-Ukrainian Road Map was signed, which clearly defined areas of cooperation in the preparation of EURO 2012. These included transport links, coordination in the field of information safety and coordination of medical support.[141]

Safety and security working groups can help partnering countries to develop common or similar safety and security standards, provide compatible planning, management, and training of operational staff, and establish channels for the proper exchange of information.

## LEGACY CONSIDERATIONS

**Security measures that last beyond the life cycle of the MSE: Technology, infrastructure and practices**

MSEs can be a platform for the development of security technologies in major urban centres, making MSEs “laboratories” for introducing new security systems.

**Example – Poland UEFA Euro 2012**

The organizers of Poland 2012 implemented the following security measures for the competition, which lasted beyond the life cycle of the MSE, and are integrated into communities and cities:

- Antiterrorist security systems for stadiums and their surroundings;
- An integrated crowd control system;
- Audio-visual recording of crowd behaviour;
- Training for stewards;
- CCTV systems for public institutions and municipalities;
- Vehicle and person recognition systems.[142]

[141] Liedel, K., & Piasecka, P. (2012). EURO 2012 Security as a Joint Task of Poland and Ukraine – A Challenge for National and International Security Systems. *POLISH-UKRAINIAN BULLETIN*, pp. 41-54.

[142] See https://www.statewatch.org/media/documents/analyses/no-207-major-events-public-order.pdf .

## - Russian Federation

**Special Law for the FIFA World Cup™ and UEFA 2020 MSEs**

In June 2013, the Russian Federation enacted a Federal Law regarding preparation and hosting of the 2018 FIFA World Cup Russia™, the 2017 Cup of Confederations, the UEFA 2020 championships and modification of separate legal acts of the Russian Federation.[143] This law integrates applicable regulations relevant to the planning, organization and implementation of the FIFA and UEFA MSEs. The law covers several aspects related to the security of MSEs, including entry into the Russian Federation, departure and migration registration, safety matters in connection with the implementation of activities for the FIFA and UEFA events, development of communication and information technologies and regulation of urban planning activities.

**Example – The 2018 FIFA World Cup™ in the Russian Federation:**
**Necessary steps to configure and secure event systems and infrastructure**

From the planning perspective, organizers should leverage best practices of private-sector partners to develop and incorporate appropriate measures to prevent or respond to cyberthreats. (See Chapter II of the Guide, box on cyberattacks)

Based on lessons learned from the 2018 FIFA World Cup Russia™, which was the target of a variety of cyberattacks, necessary steps to better configure and secure event systems and infrastructure were developed:

- Gathering threat intelligence before, during, and after the event to assess the security landscape and potential threats;
- Implementing proper access controls to manage the flow of information and prevent any intrusions into servers and endpoints;
- Checking systems and applications for vulnerabilities will help determine what needs to be updated or fixed on a real-time basis;
- Setting up security compliance audits and certification on contractors or supporting organizations to minimize possible weak points that threat actors can attack;
- Training all personnel on cybersecurity basics, especially if they are responsible for important systems; and
- Implementing a cyberattack response and recovery plan to deal with the aftermath of incidents, including worst-case scenarios.[144]

## THE SECURITY PLANNING

**Responsibility Accountability Matrix (RAM)**

Whenever planning an event that involves international collaboration, it is imperative to implement a means to define organizational and individual roles, responsibilities, and expectations early on to avoid misunderstandings and controversies. The use of a charting system known as a Responsibility Accountability Matrix (RAM) in the planning process that is agreed upon and signed off by all participants, serves to determine and assign specific individuals or agencies to be responsible and/or accountable (financial and service delivery) for various deliverables required for the event. It also ensures broad understanding of processes and relationships and helps when there is a need for conflict resolution.

**Example – 2018 FIFA World Cup Russia™**

During the 2018 FIFA World Cup Russia™ in the Russian Federation, RAM, a detailed matrix emphasizing multi-stakeholder partnerships and dialogue, was created. The matrix defined a clear division of responsibilities and the use of public and private security companies.

[143] See https://cis-legislation.com/document.fwx?rgn=60361 .

[144] *Sporting Event Threats*, 2018; see https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sporting-event-threats-lessons-from-the-2018-fifa-world-cup .

The matrix comprised three pillars:

- The role of volunteers and the right number of volunteers required;
- The use of public-private partnerships (PPP) to deal with the financial requirements of the MSE; and
- The dialogue between different stakeholders (i.e. public and private, federal, and local, stadium and cities, coordination between the different security services, etc.) to come to an agreement on the repartition of responsibilities and each entities requirements.[145]

**Volunteers - 2018 FIFA World Cup Russia™: Human and material resources**

It will be essential to identify what human resources will be needed at which moment in time and also to identify the degree of expertise in leadership and management roles required. Identifying and selecting sufficient and skilled human resources for the operational delivery of an MSE will be a significant task, requiring considerable coordination from a planning perspective. The Local Organizing Committee will manage their recruiting drives for both salaried staff as well as volunteers. A portion of the LOC volunteer cadre can be shared with the security team to perform appropriately related security duties.

During the 2018 FIFA World Cup Russia™, an important element of its success was the contribution of vast numbers of volunteers who were well trained and integrated.[146]

## LEGACY CONSIDERATIONS

**Example – Russian Federation: The use of stewards in collaboration with sports federations in favour of security (especially crowd management)**

The Russian Federation trained 16,500 stewards prior to the 2018 FIFA World Cup Russia™ in crowd management. These trainings were based on experience gained during European football competitions such as UEFA EURO tournaments, the UEFA Champions League, and the UEFA Europa League.[147]

## • State of Qatar

## FOUNDATIONS OF SECURITY AT MAJOR SPORTING EVENTS

**Proper Estimate of Security Costs**

In light of the substantial size of security-related budgets and their impact on the overall budget of the event and the economy of the Host Authority, a careful and realistic estimate of costs is an essential step for a country to self-assess its capacity to host an MSE.

With the emergence of new and complex threats, security costs associated with organising an MSE have risen in recent years,[148] increasing the need to engage in meticulous budget calculations. A careful approach is required to assess the security costs of previous MSEs against the likely costs of the new event.

[145] Source: Expert interview, April 2020.

[146] See https://resources.fifa.com/image/upload/yjibhdqzfwwz5onqszo0.pdf and expert interview.

[147] See https://tass.com/sport/968754 .

[148] Richard Giulianotti and Francisco Klauser (2010), "Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda", *Journal of Sport & Social Issues* 34 (1); see https://www.researchgate.net/publication/43108443_Security_Governance_and_Sport_Mega-events_Toward_an_Interdisciplinary_Research_Agenda .

Budgeted Security Costs as per Bid Evaluation Reports for the 2018-2026 period

- Qatar 2022: US$ 61.8 million
- Morocco 2026: US$ 11 million (Note: budgeted safety and security costs of US$ 11 million were considered lower than the baseline, whereas the budgeted Safety and Security Costs of US$ 99 million in the United Bid 2026 were considered higher than the baseline.[149])
- United Bid (Canada, United States, Mexico) 2026: US$ 99 million

## POLITICAL, ECONOMIC AND SOCIAL DIMENSIONS OF MAJOR SPORTING EVENTS

### Qatar Vision 2030

Political and economic developments have given rise to the use of sports diplomacy as an instrument of soft power. Since the times of ancient Greece, sport has been an instrument used in the game of nations. One recent example of the use of such soft power is the strategic focus that Qatar decided to give to the potential of sport to serve diplomatic purposes, but also for improving national health and to facilitate economic and eco-sustainable modernization, diversification and attractiveness, away from the traditional gas and oil sectors.[150] Two years before Qatar won the bid to host the 2022 World Cup, Qatar's leadership unveiled Qatar National Vision 2030.[151] The hosting of sports tournaments aims to be leveraged to showcase ideals of modernity, proficiency and innovation and is intended to frame the state as a cooperative, responsive and friendly member of the international community, seeking to align itself to universal ideals of peace and security.

Sports have been positioned as a central element in Qatar Vision 2030 and serve as a catalyst for human, social, economic, and environmental development of the country. Sport is also a tool to foster international dialogue and provide care within the framework of broader programmes in the field of international development and cooperation. In line with this vision, several major sporting events have been hosted by Qatar since 2006. Some are currently in the planning phase, such as the FIFA World Cup Qatar 2022™, the first World Cup to be held in the Arab world.

Sports are an integral part of Qatar's identity and play a major role in the way the country plans to grow and keep developing as a peaceful nation, open, free, and aligned to international human rights standards. The value of sports culture in Qatar is reflected in the launching of local initiatives such as the National Sports Day, an official public holiday, and the 'Doha Goals' initiative, the world's premier platform for world leaders to create initiatives for global progress through sports.[152]

### Example – Security Feedback in the FIFA Bid Evaluation Reports

The Russian Federation, in its Bid for the 2018 FIFA World Cup™, presented a security concept outlining a "Safe City" initiative, integrating human factor elements (recruitment and training of high-calibre officers) with best practices and smart technologies. The bid identified four principles as benchmarks for success: friendliness, faith, force and moving forward. Whilst the Russian Federation submitted comprehensive and well-structured security information, FIFA, in its Bid Evaluation Report, concluded that international safety and security standards were only "likely" to be met.

FIFA applies a robust evaluation model to assess Bids. It issues a Bid Evaluation Report to each bidding Government, addressing weaknesses and gaps of the security strategy, based on the information provided. For the 2022 FIFA World Cup Qatar™, it was pointed out that the challenge of ensuring

[149] 2026 FIFA World Cup™ Bid Evaluation Report; see https://resources.fifa.com/image/upload/bid-evaluation-report-2026-fifa-world-cuptm.pdf?cloudid=ir3g14juxglqbbteevvf .

[150] Middle East Institute; see https://www.mei.edu/publications/qatars-soft-power-sports-diplomacy

[151] Qatar National Vision 2030.

[152] Doha GOALS, see http://www.dohagoals.com/en/home .

effective crowd management was not addressed in sufficient detail. However, Qatar's compact World Cup concept was considered a security advantage.

The 2026 World Cup is to be co-hosted by Canada, Mexico and the United States. This will be the first World Cup to be co-hosted by a trio of geographically connected nations. In contrast to a single nation, such as Qatar with only one point of entry via Hamad International Airport, FIFA in its 2026 Bid Evaluation Report stated that there were still some questions to be answered in relation to how the three North American countries would ensure cross-border integration, cooperation and consistency from a security standpoint.

In the overview of the scoring system for the technical evaluation of the 2026 bids, FIFA mentions security briefly as a sub-criterion related to the FIFA Fan Fest. The emphasis of the report focused on infrastructure and the commercial side of the event. In FIFA's Guide to the Bidding Process, the issue of security wasaddressed once only in a two-sentence paragraph under Government Support.

The Bid Evaluation Report for the 2023 FIFA Women's World Cup™, revealed that the Australia and New Zealand's bid provided a substantial level of detail regarding security, including how the two Governments and their security agencies would cooperate in the planning and delivery of the tournament through the use of dynamic risk assessments.[153]

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Laws on Private Security and Counterterrorism

Qatar has legislation in place to ensure planning, organization and implementation of major sporting events and is currently in the process of adapting its laws and strategies to integrate FIFA requirements in terms of stadiums, facilities, logistics and publicity in anticipation of the FIFA World Cup Qatar 2022™.

The country has already in place specific legislation Regulating the Provision of Private Security Services (Law No 19 of 2009)[149] which provides the basis for action by private security companies, including those who will be engaged in the security of the FIFA World Cup Qatar 2022™. The Law establishes that the relationship between private security companies and the service provider will be governed by a contract agreed between the parties and that private security services shall be performed in full compliance with Qatar´s laws.

These Laws on MSEs are complemented by Qatar's new regime to combat terrorism under Law No. 27 on Combating Terrorism of 27 December 2019. The law enhances penalties for terrorist offences, provides a definition of terrorism, increases prosecutors´ investigative capabilities and establishes the Qatar National Counter-Terrorism Committee[154], which is in charge of coordinating anti-terrorism

[153] 2018 FIFA World Cup™ Bid Evaluation Report: Russia, see https://img.fifa.com/image/upload/mjwq4omnm58mcbwzd2pt.pdf ; also, Bidding process for the 2026 FIFA World Cup™. Overview of the scoring system for the technical evaluation of bids. See https://resources.fifa.com/image/upload/overview-of-scoring-system-for-the-technical-evaluation-of-2026-fifa-world-cup-b.pdf?cloudid=eg1fnzj6q9ik5gmggkwi . Guide to the Bidding Process for the 2026 FIFA World Cup™;
see https://img.fifa.com/image/upload/hgopypqftviladnm7q90.pdf . The FIFA Women's World Cup 2023 Bid Evaluation Report, see https://resources.fifa.com/image/upload/fwwc-2023-bid-evaluation-report.pdf?cloudid=hygmh1hhjpg30lbd6ppe .

[154] See https://portal.moi.gov.qa/wps/portal/NCTC/Home/!ut/p/a1/dY1Nb8IwEER_ja_ZLTQhcKPhI6IBFBQJ8KVyJBMskqyxF_j7pQgOCDq3GT3NAwkbkK06m0qxoVbVf11GP2Gajaef37iIJ7MQ82WejdJ-

efforts carried out by several government bodies, the implementation of the obligations contained in the resolutions of the UN Security Council and other obligations related to combating terrorism.[155]

## THE SECURITY PLANNING SYSTEM

### Security Design

### Example – FIFA World Cup Qatar 2022™

The Supreme Committee for Delivery and Legacy (SC) was formed to deliver Qatar 2022. The SC established a security department (hereinafter also Security Team) comprised of professionals who had been involved in security design for other international MSEs. The Security Team established guidance documents detailing international best practices and developed their vision of how security was to be implemented in the design of the stadiums. The Security Team vetted security designers to guarantee that Suitably Qualified and Experienced Persons  would be working on the project.

The Security Team provided a national threat assessment to security consultants for use in security risk assessments. The threat assessment included technical security mitigation measures completed for each stadium and formed the basis of security design for a stadium.

Throughout the different design stages, the Security Team engaged with security consultants and national security stakeholders to review the designs and suggest improvements. Contractors finalised the designs put forward by the engineering consultancies, and the Security Team managed to arrange implementation by the contractors.

By designing security and using experienced people on both the consulting and client sides, an effective security design was achieved for multiple stadiums pursuant to international best practices.[156]

- **South Africa**

## POLITICAL, ECONOMIC AND SOCIAL DIMENSIONS OF MAJOR SPORTING EVENTS

Despite the difficulty in accurately evaluating the real economic costs of hosting an MSE, and regardless of the fact that in recent years many citizens have come to look at MSEs with an increasingly skeptical eye, it is undeniable that MSEs have repeatedly obtained international, and at times even geopolitical relevance. MSEs also offer opportunities to promote positive change within a hosting country as well as for the international community at large. MSEs have social, political and diplomatic dimensions, offering an opportunity to strengthen international dialogue.

### Example – South Africa Rugby World Cup 1995

During the 1995 Rugby World Cup, Nelson Mandela (Madiba) showcased the power of sport to unite people in addition to redefining a country’s international image. The Rugby World Cup served as a vehicle for reconciliation - strengthening social cohesion and healing wounds among a nation that suffered from deep socio-economic divisions. Madiba understood what sport meant to the South African people and used it in such a way that all communities felt they belonged to South Africa equally – he used sport to build the nation. As Madiba said: “Sport has the power to change the world. It has

3sVlBGuQz8i0V3xdkU5aRKu0g_hxB_CfDBFmIKuayptuO2zLblyBdHqnnXbByV3nPbP1A4ECLTlWddCQCSo6B0cl8GL9Yxe4SIpEoCrpxAk1jWHWWqDT3lLrTWlqw0b7d6I9eYbNyz_Yw2E353D7C4qIiII!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/

[155] See https://blogs.loc.gov/law/2020/03/falqs-qatars-new-counterterrorism-law/ .

[156] See https://www.qatar2022.qa/en/about .

the power to inspire. It has the power to unite people in a way that little else does. It speaks to youth in a language they understand. Sport can create hope where once there was only despair."[157]

## POLITICAL, ECONOMIC AND SOCIAL DIMENSIONS OF MAJOR SPORTING EVENTS

- **Information Management Information Technology (IMIT)**

Several stand-alone and collaborative digital technology platforms ought to be used throughout the MSE planning environment. Planning safety and security measures for MSEs requires reliance on spatial data and geographical reference maps to define resources and physical security requirements. This holds true for major sports events in particular, but also becomes a requirement for the overall management of transport systems, logistic operations, and traffic generated by the major event itself. A key tool to address this challenge is Geographical Information System (GIS) technology. This enables overlaying safety and security measures with increased accuracy and allows for managing and monitoring these during the event in real-time. GIS technology allows the integration of spatial information into a single, holistic picture, whereby a dynamic, common operating map is created to enable everyone to see the same information and deploy resources accordingly.[158]

### Example – GIS Technology: the 2010 FIFA World Cup South Africa™

The practical use of GIS technology for the safety and security planning of the 2010 FIFA World Cup South Africa™ was embedded within the Johannesburg Metropolitan Police Department (JMPD). GIS technology captured all relevant event-related information into a spatial geodatabase which included:

- Transportation hubs and routes
- Temporary facilities (e.g. park and rides, park and walks, rail stations, bus stations)
- Security layers (e.g. traffic warning zone, traffic-free zone, inner perimeter, stadium perimeter)
- Road closures (e.g. traffic control points, vehicles permit checkpoints)
- Permanent structures (e.g. stadiums)
- Temporary overlays (e.g. fences and bags screening areas), and
- Police officers' deployment for traffic management purposes.

Spatial-related information supported the development of accurate documentation related to event safety and security measures and the traffic management plan from which residents and businesses benefitted. GIS was utilized for communicating FIFA World Cup™ related information to the public.

## LEGACY CONSIDERATIONS

### Social Transformations and Changes in Inter-Community Relations

The goodwill generated by including local communities in MSE planning constitutes a form of social capital which can last for a long time.

MSEs can offer an opportunity to empower underprivileged sectors of society and counteract threats like the violent radicalization of vulnerable youth. The jobs, infrastructure improvements, financial investments, and profit-sharing programmes that are often generated as part of an MSE can improve the economic and social outlook of members of disadvantaged communities. More direct activities can also play a role: during the 2010 FIFA World Cup South Africa™, FIFA organized a football competition where local youth could experience the atmosphere of a major sporting event in a safe and fun-filled environment of goodwill and fair play. Moreover, the event engaged the support of other NGOs to offer free HIV tests and other community services.

[157] See https://www.sportanddev.org/en/article/news/nelson-mandela-and-power-sport .

[158] Pispia, Giovanni. (2015). A Case Study Analysis on the Implementation of GIS Technology for Safety and Security Planning during Major Sport Events. See https://www.researchgate.net/publication/333827308_A_Case_Study_Analysis_on_the_Implementation_of_GIS_Technology_for_Safety_and_Security_Planning_during_Major_Sport_Events .

- **Spain**

## LEGACY CONSIDERATIONS

### Urban Regeneration

The organization of an MSE can become the starting-point to facilitate urban development or regeneration. Clearing slums, combined with the offering of alternative housing for those affected, can become a lasting legacy for the local community.

### Example – The Olympic Games of 1992 Barcelona

The impact of the Olympic Games on urban regeneration is one of the pillars with regards to sustainability which in return impacts on a lasting legacy for the community. The 1992 Summer Olympic Games in Barcelona was one of the most important urban transformations that the city has undergone throughout its history, and a good example of the impact that hosting an MSE can have on cities or countries. The Games brought with it the opportunity to transform run-down, derelict and industrial areas. The ambitious strategies to redevelop and regenerate Barcelona have been commonly associated with a ”Barcelona model”, heralded for delivering urban renewal across other cities.

Acting as a catalyst to deliver the necessary infrastructure required to regenerate, the city’s Olympic Games investment programme included: the renovation of the Olympic stadium and construction of a sports pavilion; building a motorway ring and highway infrastructure; delivering 4,500 new housing units; extending the airport; delivering new cultural facilities; and renewing 110 hectares of parks and 5km of new beaches. In the lead up to the Games, the ring roads project was accelerated and managed to reduce traffic in the city centre by 15 per cent. The ring roads defined a new urban reality that confirmed Barcelona’s change of scale, its transformation from a city to a metropolis. Whilst the Olympic Park is now a popular tourist destination, the waterfront and Poblenou (Industrial) areas provide prominent examples of how the Olympic Games were used as a tool to deliver regeneration across the city. The Games also contributed to the city’s establishment as a touristic hub in Spain and Europe (1.7 million visitors in 1990 increasing to over 6 million over the next 14 years) which in turn created an economic boom and important infrastructural changes to cater to larger crowds. [159]

### The 2019 Champions League final in Madrid - Fan Information Teams (FIT)

Visitors and spectators: Consulting prospective spectators, by reaching out to them through social media, supporters’ organisations or through other channels, may provide useful feedback for security arrangements since these often involve direct interaction with spectators from prior events, such as procedures at border entries, on-site security checkpoints, or fan zones. Spectators may be able to offer practical ‘on-the-ground’ suggestions for improving safety and security measures.

### Example – The 2019 Champions League final in Madrid - Fan Information Teams (FIT)

At the 2019 Champions League final in Madrid, fan zones separating rival team supporters were patrolled by Fan Information Teams (FITs). Theseteams, which included police officers and representatives from clubs’ supporter associations, interacted directly with fans to solve problems and gather information. [160]

[159] Barcelona Field Studies Centre; see https://geographyfieldwork.com/OlympicLegacies.htm .

[160] Badcock, J., and T. Morgan. :Police Plan Unprecedented Security Operation for “High Risk” Champions League Final:, *The Telegraph*, 28 May 2019; see https://www.telegraph.co.uk/football/2019/05/28/police-plan-unprecedented-security-operation-high-risk-champions/ .

- **Ukraine**

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Specific laws to secure football matches

In preparation of the UEFA European Football Championship in 2012, Ukraine enacted a specific law that included several of the international standards analysed in the previous sections. The Ukrainian Law ensuring public order and safety in connection with preparation and holding of football matches[161] aims at integrating under one umbrella all other relevant regulations in the field of sport security- and it establishes a list of security-related technical and organizational requirements for football stadiums. It mainly focuses on stadium-security organizational requirements, which have to be individually developed for each stadium. Additionally, it delineates the responsibilities of football match organizers, stadium owners, football clubs, stadium (football club) security services, as well as the rights and obligations of spectators.

According to the Law, the organizer of the football match, the owner of the stadium and the football club are responsible for venue security, while police are in charge of non-venue security, including evacuation routes, transport routes and the like. Police may also ensure public order inside the stadium if required. The Law includes provisions for the establishment of coordination groups for each game, to ensure proper cooperation between all stakeholders involved in the organisation of football matches.

### Arena Lviv, Ukraine Technology for UEFA Euro 2012[213]

| | |
|---|---|
| **Investment model** | Publicly financed and state-commissioned new stadium built.<br>Part of a self-sustaining sports and entertainment facility project. |
| **Operational Challenges** | Meeting UEFA stadium requirements.<br>Protected seating for 35,000 spectators, 450 VIP boxes, concert halls, public fan-zones, and underground car park.<br>Avoid over-intrusive police presence.<br>Control the number of people entering the stadium.<br>Provide round the clock surveillance of facilities.<br>Integrate the stadium's surveillance system with its central management suite.<br>Help ensure the comfort of visitors and transform fan experience in a positive way. |
| **Technical Requirements** | Manage to expand video systems in terms of number of cameras, storage, multiple remote locations, and bandwidth constraints.<br>Provide secure access to users, from any location, to enhance collaboration.<br>Support various vendor devices (cameras, encoders, access control systems) and applications (command and control, video analytics).<br>Integrate video with other networked applications.<br>Use a wireless network to deploy a cashless payment system to reduce queuing at electronic point-of-sale terminals. |
| **Technology Solutions** | Video systems management platform for secure, policy-based access to live and recorded video.<br>Wi-Fi access points.<br>Video Surveillance IP Cameras deployed outside and inside the stadium.<br>Physical security software comprising data, voice, video, safety and security, digital signage, point-of-sale, and building management on a single Internet Protocol (IP) platform.<br>Digital media players, communication gateways and transformation devices. |
| **Results** | Enhanced protection of people and assets, from a centralised location.<br>Wide acclaim for secure and expert management of spectators/ crowds. |

[161] See https://cis-legislation.com/document.fwx?rgn=46091 .

| | |
|---|---|
| | “Future-proof” integration compatibility with third-party video analytics applications.<br>Multi-purpose equipment can be adapted and customised for future events.<br>Business expansion opportunities via increased interest from advertisers and sponsors. |
| **Future Possibilities** | Expand video system platform to integrate video analytics applications and surveillance feed analysis programs without the need for a significant amount of equipment technology or infrastructure upgrades. |

## CO-HOSTING MAJOR SPORTING EVENTS

**Set up joint preparations well in advance, including the establishment of agreements between governments and relevant multi-national working groups involved**

As an example, in 2008 the Government of Poland and the Cabinet of Ministers of Ukraine signed an agreement for cooperation for the organisation of EURO 2012, including the planning of safety and security. In 2010, a Polish-Ukrainian Road Map was signed, which clearly defined areas of cooperation in the preparation of EURO 2012. These included transport links (air, road, and rail), coordination in the field of information safety and the coordination of medical support.[162]

- **United Kingdom of Great Britain and Northern Ireland**

## FOUNDATIONS FOR SECURITY FOR MAJOR SPORTING EVENTS

**The overarching vision of the London Olympic and Paralympics: leadership and vision**

In order to achieve the security mission of an MSE, several goals or strategic objectives, critical to the planning process, need to be brought together in a synchronised manner. Each event is uniquely different; therefore, organizers and planners, based on their specific environments, must determine what it is they want to achieve to accomplish their mission.

**Example – The London 2012 Olympic Games**

The overarching vision of the London Olympic Board for the 2012 Olympics and Paralympics was "To host an inspirational, safe and inclusive Olympic and Paralympic Games and leave a sustainable legacy for London and the UK". From that, the safety and security functional areas developed their strategy with the overall aim being “To deliver a safe and secure Games, in keeping with the Olympic culture and spirit.”

They determined the objectives needed to achieve their aim:

- Protect Olympic and Paralympic venues, events and supporting transport infrastructure, and those attending and using them;
- Prepare for events that may significantly disrupt the safety and security of the Games and ensure capabilities are in place to mitigate their impact;
- Identify and disrupt threats to the safety and security of the Games;
- Command, control, plan and resource (C2PR) the safety and security operation; and
- Engage with international and domestic partners and communities, to enhance our security and ensure the success of our Strategy.

All these operational outcomes could only be achieved by putting in place the right capabilities, using them effectively and in an integrated manner with the other critical domains upon which the overall

[162] Liedel, K. and Piasecka, P. (2012). EURO 2012 Security as a Joint Task of Poland and Ukraine – A Challenge for National and International Security Systems. *Polish-Ukrainian Bulletin,* pp. 41-54.

delivery of the Games depended, notably transport, government operations, city operations and Games operations.[163]

## LEGAL AND INSTITUTIONAL FRAMEWORKS

### Legislation to counter hooliganism and terrorism

Apart from terrorist threats, hooliganism has posed significant challenges for the British Government in the past few decades which have been addressed through the adoption of legislation which benefited the organization of national routine sporting competitions and MSEs. To mitigate hooligans´ activities, the Government enacted several statutes referring to supporters but also organizers of MSEs, e.g., the Football Spectators Act 1989,[164] the Football (Offences and Disorder) Act 1999,[165] the Violent Crime Reduction Act 2006,[166] and the Sports Grounds Safety Authority Act 2011.[167] These Acts include several measures aimed at managing large crowds and countering hooliganism, such as:

- Use of sports-related offences databases;
- Prohibitions against leaving the territory and detention in police custody;
- Creation of specific offences, such as entering a stadium when drunk or in possession of alcohol or throwing any objects at or towards the pitch;
- Using fireworks, racist chanting; and
- Measures to ensure that all spectators are seated to deal with the risk of crowd crushing.

These specific regulations on MSEs are complemented by various guidelines aimed at countering terrorism. For instance, the Crowded Places Guidance[168] notes that the United Kingdom faces a real threat from terrorism and crowded places, such as shopping centres, sports stadiums, bars, pubs and clubs.

The Cyber Security for Major Events[169] outlines how to incorporate cyber-risk management processes into major event planning. It is aimed at organizations running large-scale sporting events, but the steps and procedures outlined can be incorporated into general event planning. The Guidance mentions that major events are increasingly reliant on digital systems and technology and that cyberattacks affecting the confidentiality, integrity or availability of these systems can have a disruptive impact, resulting in financial and reputational damage.

## STAKEHOLDER COOPERATION

### Inter-agency cooperation

Successful inter-agency cooperation largely relies on a robust command and control structure with a clear delineation of leadership roles, decision-making processes, and responsibilities of each governmental agency in the early planning process. For example, in the lead up to the London 2012 Summer Olympics, inter-agency exercises were held to test inter-agency responses to emergency incidents. However, in one of the scenarios around the torch relay, it became apparent that participants did not know whose responsibility it was to divert the torch relay in case of a fire. While such a lack of clarity can cause confusion during preparatory exercises, it could be more serious in a real emergency incident.

[163] London 2012 Olympic and Paralympic Safety and Security Strategy; see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97983/olympic-safety-security-strategy.pdf .

[164] See https://www.legislation.gov.uk/ukpga/1989/37/contents .

[165] See https://www.legislation.gov.uk/ukpga/1999/21/contents .

[166] See https://www.legislation.gov.uk/ukpga/2006/38/contents .

[167] See https://www.legislation.gov.uk/ukpga/2011/6/contents/enacted .

[168] See https://www.gov.uk/government/publications/crowded-places-guidance .

[169] See https://www.ncsc.gov.uk/guidance/cyber-security-for-major-events .

Furthermore, printed and online documentation, including guidebooks and written agreements, are very useful in enhancing inter-agency collaboration. For example, the UK's Green Guide[170] and Purple Guide[171] are UK government-funded guidance books on spectator safety at sports grounds and identify the professionals and services that are accountable for making decisions. The use of codified principles and procedures between various agencies make the roles and responsibilities of the leading organisation more explicit and facilitate inter-agency collaboration (See Chapter VII on Security Planning).

**Private Companies Engagement**

Where goods, services and assets can be shared, it makes sense to utilize the most efficient and effective procurement routes as long as the required legal, ethical, economic and moral standards can be met. It is vital that applicable international trade agreements be respected when using public sector procurement processes (see Chapter V on Legal and Institutional Frameworks).

Open and transparent procurement processes must be established with robust auditing and public scrutiny mechanisms. Illicit opportunities for organised crime to infiltrate the supply chain and provide counterfeit or sub-standard building materials are often found with sizeable multi-year construction projects. Due consideration should also be given to labour-related issues with long-term building ventures.

**Example – London 2012 Olympic Games – Private Companies Engagement**

In preparation for the London 2012 Olympic Games, the British Security Industry Association held regular briefings for its members and dedicated an area of its website to the Games that provided commercially useful information and kept its members informed on developments and opportunities. [172]

## VIII. COMMUNICATION STRATEGIES

**Civil Society: Example – London 2012 Olympic Games and My Dream 2012**

In the leadup to the London 2012 Olympic Games, a communications campaign, My Dream 2012, was put in place to offset a growing narrative that the Games were "un-Islamic", since coincided with the holy month of Ramadan. The campaign, which included documentary film and radio, featured Muslim athletes competing in the Games and was a key means of reaching out to Muslim communities.[173]

## THE SECURITY PLANNING SYSTEM

The lead security agency and critical infrastructure stakeholders, must conduct threat and risk assessments of event venues and important non-venue sites. Information should also be gathered from open-source, real-time data on suspect activities, or covert operations long before the event takes place. Intelligence sources must produce timely and accurate reports throughout the event planning phase to ensure plans and mitigation strategies evolve to meet security threats to the MSE.

A good example of a security planning system was the London 2012 Olympic Games, where the U.K. Government set up a specific methodology to identify the types and relative levels of risk which could have hindered the effective delivery of a safe and secure MSE, thereby informing strategic-level decision making and planning.[174]

[170] See https://www.eventsindustryforum.co.uk/index.php; see also https://sgsa.org.uk/greenguide/; and https://www.thestadiumbusiness.com/2018/11/05/sgsa-publishes-updated-green-guide-stadia/ .

[171] See https://www.thepurpleguide.co.uk/ .

[172] Silke, Andrew, et al. *Terrorism and the Olympics: Major Event Security and Lessons for the Future*. Routledge, 2010.

[173] Expert Group Meeting on the Security of Major Events, February 2020, New York.

[174] See Olympic Safety and Security Strategic Risk Assessment (OSSSRA), U.K. Home Office, 2011.

### Integration Among Organizers

Regarding the integration among Games organizers, which is found to be a key challenge, one of the British Organising Committee of the Olympic Games IOCV Final Report findings indicated that:

> "The key is to avoid function and stakeholder groups operating in "silos" and failing to collaborate and communicate with each other effectively. OCOGs [Organising Committee of the Olympic Games] have a responsibility to instil an organisational culture among all partners and stakeholders that encourages improved integration and communication, as well as to find new ways of promoting awareness and understanding of the different interfaces between Games organisers".[175]

.

- **United States of America**

## COMMUNICATION STRATEGIES

### Social media and the 2013 Boston Marathon Bombings

Social media have become a powerful tool for reaching diverse audiences, including when it comes to conveying security measures. through frequent communication on social media platforms, the LOC can maintain a constant dialogue with the public, and thereby build trust in the community, which enhances security.

The two bomb attacks of 15 April 2013, which killed three people and injured many others during the Boston Marathon, have shown that social media played an integral part in the response – especially for those on the ground. Many of those impacted used Facebook and Twitter to get updates and send messages to their families and friends. It was also an opportunity for security and venue staff to share confirmed information about situation details and safe exit routes. After the bombings, some family members were notified by their loved ones via Twitter before the bombings even received major media attention.[176]

# Multiple Countries Bids

- **United Bid of Canada, Mexico and United States of America**

## FOUNDATIONS OF SECURITY AT MAJOR SPORTING EVENTS

### Proper estimate of security costs

A careful and realistic estimate of costs is an essential step for a country to self-assess its capacity to host an MSE. With the emergence of new and complex threats, security costs associated with organizing an MSE have steadily risen in recent years,[177] thus increasing the need to engage in meticulous budget calculations. A careful approach is required to assess the security costs of previous MSEs against the likely costs of the new event.

[175] International Olympic Committee, Final Report of the IOC Coordination Commission. 2010, See https://stillmed.olympic.org/media/Document%20Library/OlympicOrg/Games/Summer-Games/Games-Beijing-2008-Olympic-Games/Final-Report-of-the-IOC-Coordination-Commission/Final-Report-of-the-IOC-Coordination-Commission-Beijing-2008.pdf .

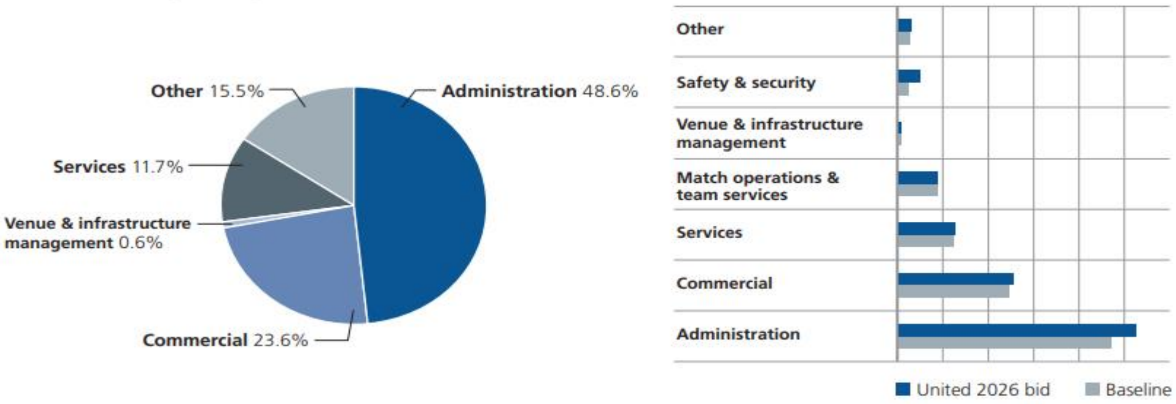
[176] Phillips, Ted. "Boston Marathon Bombing Reaction Unfolds on Facebook, Twitter Updates", *Newsday*, 16 Apr. 2013; see https://www.newsday.com/news/nation/boston-marathon-bombing-reaction-unfolds-in-facebook-twitter-updates-1.5078588 .

[177] Richard Giulianotti and Francisco Klauser (2010), "Security Governance and Sport Mega-events: Toward an Interdisciplinary Research Agenda", *Journal of Sport & Social Issues* 34 (1); see https://www.researchgate.net/publication/43108443_Security_Governance_and_Sport_Mega-events_Toward_an_Interdisciplinary_Research_Agenda .

**Budgeted Security Costs as per Bid Evaluation Reports for the 2018 – 2026 period**

- Qatar 2022: US$ 61.8 million
- Morocco 2026: US$ 11 million (Note: budgeted Safety and Security Costs of US $11 million were considered lower than the baseline, whereas the budgeted Safety and Security Costs of US$ 99 million in the United Bid 2026 were considered higher than the baseline.[178])
- United Bid (Canada, USA, Mexico) 2026: the US$ 99 million

FIFA's organising costs



Overall projected organising costs per area in %

Projected organising costs v. baseline

## STAKEHOLDER COOPERATION

**Foundations for effective stakeholder cooperation**

A very important element to support the various forms of stakeholder cooperation is a shared understanding of, and respect for, human rights. There is an obligation among all members of the United Nations to protect people within their jurisdiction from arbitrary interference with their human rights. These rights, which are safeguarded in international human rights treaties, include the right to life, security of the person, the right not to be tortured, the right not to be arbitrarily arrested, the right to a fair trial, the right not to be discriminated against, the right to freedom of association, the right to freedom of expression, the right to work, the right to health, the right to recreational activities and cultural activities, among others.[179]

**Example – United Bid of Canada, Mexico, United States**

The report produced on behalf of the winning 'United' bid from Canada, Mexico and the United States outlined several human rights issues that must be considered in a transnational context, including:

- The free movement of workers, fans, spectators, journalists, and players between countries
- Cross-border human trafficking related to increased demand for cheap labour and sexual exploitation
- Embedding human rights considerations into policies and operational procedures of law enforcement agencies and private security providers
- Devising an integrated framework of grievances and remedy mechanisms to address human rights breaches.[180]

[178] 2026 FIFA World Cup™ Bid Evaluation Report. See https://resources.fifa.com/image/upload/bid-evaluation-report-2026-fifa-world-cuptm.pdf?cloudid=ir3g14juxglqbbteevvf .

[179] See the United Nations International Covenant on Civil and Political Rights (1966) and the United Nations International Covenant on Economic, Social and Cultural Rights (1966), as well as the various regional instruments.

[180] See https://img.fifa.com/image/upload/w3yjeu7dadt5erw26wmu.pdf .

## CO-HOSTING MAJOR SPORTING EVENTS

### Design a harmonized border control framework

Harmonized border control systems can simplify international cooperation between security personnel while also enhancing visitors' experience. For example:

- In preparation for the ICC Cricket World Cup West Indies 2007, the Prime Ministers of the Caribbean Community (CARICOM) designated the nine host venues as "one domestic space" for the duration of the Games, eliminating the need for people to be processed through Customs and Immigration when travelling between these countries. Also, rather than requiring individuals to acquire visas for entering each country, a single CARICOM visa was created for the duration of the event. [181]
- Similarly, during EURO 2008, hosted by Switzerland and Austria, a simplified visa process was created to allow individuals to enter both countries with a single visa. However, because Switzerland is not a member of the European Union, border controls were still required. For EURO 2008, a temporary agreement was put in place to establish joint border patrols with personnel from both countries.
- For FIFA World Cup 2026™, the United Bid (Canada, Mexico, and the US) indicated that a task force would be established to address cross-border transport and immigration and international mobility measures through the implementation of a multi-country Fan-ID system once visitors will have obtained a visa.[182]

## • ICC Cricket World Cup

From the 1987 tournament onwards, hosting has been shared between countries under an unofficial rotation system, with 14 ICC members having hosted at least one match in the tournament. Each ”cricket-playing region" in the world is granted the opportunity to host the event. In 2006, the ICC awarded the 2011 Cricket World Cup to Bangladesh, India and Pakistan. In 2015 it was the turn of Australia and New Zealand to host, and in 2019 the event took place in England and Wales. The 2023 ICC Cricket World Cup is scheduled to be hosted for the first time completely by India. The country has co-hosted the World Cup three times in the past.

## CO-HOSTING MAJOR SPORTING EVENTS

### Harmonize security-related legislation between host nations

Coordinating legislation around security-related matters can significantly enhance security operations and improve the overall security of an event. It is recommended that organising countries harmonise legislation on event-related violence, particularly in relation to criminal penalties and the treatment and extradition of offenders. It is also recommended that host and competing countries consider legal frameworks for exchanging relevant personal data and measures to prevent high-risk supporters from travelling to an event.

For example: For the ICC Cricket World Cup West Indies 2007, the CARICOM Operations, Planning and Coordinating Staff (COPACS) was established in 2007 and ratified by all participating countries.[183]. A Regional Intelligence Fusion Centre (RIFC) as a permanent intelligence core for the management of regional intelligence and threat assessment and a Joint Regional Communication Centre (JRCC) was also created. The accomplishments of the 2007 Cricket World Cup, led to comprehensive intelligence and understanding of regional security threats, culturally relevant regional security strategies and plans, managed and financed by CARICOM, upgraded regional border security and intelligence infrastructure, innovative use of technology, and the introduction of new information and communications technology (ICT) systems.

[181] See https://www.espncricinfo.com/story/_/id/22996366/‘historic-caricom-measures-icc-cwc-2007 .

[182] See https://resources.fifa.com/image/upload/2026-fifa-world-cup-bid-evaluation-report.pdf?cloudid=yx76lnat3oingsmnlvzf .

[183] ACT No. 14 of 2007, Security Assistance (CARICOM Members States) Act, 2007.

- **UEFA**

## STAKEHOLDER COOPERATION

### Bilateral and Multilateral Agreements

Bilateral agreements may be concluded between countries, but also between organizations. For the UEFA event in 2008, both the Swiss and Austrian police agencies made joint declarations on cooperation with EUROPOL. In the Swiss case, this was an extension of their existing bilateral operational cooperation agreement, the 2004 Agreement between the Swiss Confederation and the European Police Office.[184]

### Examples – Bilateral Agreements: UEFA Euro 2008 Football Championships and the 2006 FIFA World Cup Germany™

In the lead up to UEFA Euro 2008 Football Championships, which was co-hosted by Switzerland and Austria, to implement the international exchange of data and to prevent the entry and departure of individuals prone to violence, the Swiss Federal Office of Police initiated bilateral ministerial agreements (based on existing treaties) with all nations participating in the event as well as the most important transit States.[185]

### Example – UEFA Euro 2008 in Austria and Switzerland

In advance of EURO 2008, police representatives from more than 20 countries and other international law enforcement agencies, including INTERPOL, EUROPOL, Frontex, COLPOFER and Eurojust, participated in three EURO 2008 Security Conferences of Neighbouring, Transit and Participating States.

These sessions provided a platform for a wide range of event-related security issues, including data exchange and preventing the entry and departure of perpetrators of violence. Implementation arrangements were later formalised through bilateral ministerial statements based on existing treaties with all nations participating in the EURO 2008 and the most important transit states (Swiss Federal Department of Defence, 2007).

## CO-HOSTING MAJOR SPORTING EVENTS

While most security preparations and operations for in-country events will be carried out by local authorities within the Host country, there should be some level of collaboration with co-Host nations and beyond.

Cooperative policing can be further supported by Police Information and Coordination Centres (PICCs), which deal with specific event-related security issues and should be set up in each host country and include liaison officers from participating and neighbouring countries. For example, during EURO 2008, while there were no large-scale exchanges of police between Austria and Switzerland, liaison officers from Austria were posted to Host city collaboration centres in Switzerland, and vice versa. At the request of a committee of regional police forces, Swiss authorities also requested support from outside the co-hosts' borders to help manage on-the-ground activities. As a result, both German and French police forces were deployed to Swiss Host cities to support local police.[186]

[184] Verhage, A., Terpstra, J., Deelman, P., Muylaert, E., & Van Parys, P. (Eds.). (2010). Policing in Europe. *Journal of Police Studies*, *2010/3*(16); see https://books.google.com/books/about/Policing_in_Europe.html?id=OiRTW_kc7VoC .

[185] Source: Swiss Federal Department of Defence, 2007.

[186] See https://www.dw.com/en/euro-2008-co-hosts-clear-championship-hurdles-mostly/a-3253238 .

### Memoranda of Understanding with neighbouring countries and international organizations

Establishing close cooperation with other international agencies (such as INTERPOL, FRONTEX, EUROPOL, RAILPOL and TISPOL) is also important for effective security operations. For example, during EURO 2008, officers from countries contributing to the FRONTEX external border security agency were operating both in Austria and Switzerland. Similarly, in advance of EURO 2012, Polish and Ukrainian police met with INTERPOL representatives to review security preparations and identify areas of cooperation. At the request of Polish authorities, EUROPOL provided a risk analysis to brief the respective security forces. Polish police also accessed the European database of persons banned from entering stadiums.

Safety and security working groups can help partnering countries to develop common or similar safety and security standards, provide compatible planning, management, and training of operational staff, and establish channels for the proper exchange of information:

- For EURO 2020, all 12 host nations were required to present a safety and security strategy, based on a template outlining basic security requirements set by UEFA. While not every country is expected to achieve the highest security standards, this ensures every host authority will meet the minimum standards established by UEFA.
- The Council of Europe's Standing Committee of the Convention on Spectator Violence established, in 2016, an Ad-Hoc Working Group to monitor the safety, security and service preparations for UEFA EURO 2020. This Group met every semester since then and adopted a programme of consultative visits and peer-review exercises between match police commanders, which were carried out in half of the 12 hosting countries, notably Azerbaijan, Hungary, Spain, Italy, the United Kingdom and the Netherlands.[187]

### Design a harmonized border control framework

Harmonized border control systems can add value to an event by simplifying international cooperation between security personnel while also enhancing visitors' experience.

For example: during EURO 2008, hosted by Switzerland and Austria, a simplified visa process was created to allow individuals to enter both countries with a single visa. However, because Switzerland is not a member of the European Union, border controls were still required. For EURO 2008, a temporary agreement was put in place to establish joint border patrols with personnel from both countries.

### Organize study visits to share practical experiences

For example, the Standing Committee of the Council of Europe Convention on Spectator Violence, through its Ad-Hoc Working Group on the 3S preparations for UEFA EURO 2020, organized, between 2018 and 2019, four monitoring visits and two peer-review exercises to six of the twelve organizing countries. In particular, the peer-review exercises, organised in London and Amsterdam, enabled match police commanders of the hosting cities to exchange on good practices and lessons learned on police tactics and operations, thus promoting a harmonised approach during this major event across Europe.

[187] Council of Europe: Holding monitoring visits to ensure compliance with commitments by Member States.

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

unicri
United Nations
Interregional Crime and Justice
Research Institute

UNAOC
United Nations Alliance of Civilizations

ICSS
Safeguarding Sport

# GUIDE ON THE SECURITY OF MAJOR SPORTING EVENTS

## PROMOTING SUSTAINABLE SECURITY AND LEGACIES

SPORTS