INTERPOL

PROJECT **STADIA**

Safe & Secure Major Events

A SUMMARY OF THE INTERPOL PROJECT STADIA KEY CONSIDERATIONS FOR SECURING MAJOR EVENTS

First Edition
October 2023

Contents

FOREWORD

In line with INTERPOL's vision, of "Connecting Police for a Safer World" Project Stadia set out to draw on expertise from across the globe to contribute to the planning and execution of policing and security arrangements for the 2022 FIFA World Cup in Qatar and leave a lasting legacy for the world's law enforcement community.

To further its objective INTERPOL Project Stadia hosted group meetings with experts from around the world on the key themes of physical security, legislation and cybersecurity. These meetings brought together global experts from law enforcement, event organizers, governments, the private sector, academia and civil society to explore existing and emerging knowledge, and to develop independent recommendations for planning and executing security arrangements for major international sporting events. To capture good practices and lessons learned before, during and after major international sporting events, Project Stadia conducted observation and debriefing missions with designated security officials from both the public and private sectors who had direct responsibilities for policing and security operations. Where necessary, Project Stadia engaged in horizon scanning to enrich and support the input from individual global experts and groups.

A core component of Project Stadia has been the creation of a Centre of Excellence to help INTERPOL member countries in preparations for major events. In pursuit of its goals, Project Stadia has facilitated a large number of discussions between experts on a wide range of topics related to safety, security and service for major events, in order to formalize and share recommendations via the online platform (Stadia Knowledge Management System). It has now issued this publication which consolidates all the recommendations collected through these activities over the last 10 years so that it can share the learning with its members worldwide.

In this spirit of knowledge-sharing and bringing law enforcement and other stakeholders together Project Stadia has endeavored to develop a framework of key thematic areas (chapters) that combine to present the integrated, interrelated and interdependent nature of major event safety, security and service from a strategic, tactical and operational perspective and to provide its members with a living document and knowledge repository so that they can keep pace with a rapidly changing environment.

If used in the manner in which it is intended, we believe that the information, advice, recommendations and key considerations contained within this document will improve outcomes for law enforcement agencies, other key stakeholders and the public.

FUNDING AND ACKNOWLEDGEMENTS

Funding for this 10-year project was provided by the Government of Qatar and conducted by INTERPOL Project Stadia. We give very special thanks for this research project to the members of the Project Stadia team who hosted the expert presentations, conducted the interviews, attended the international onsite event reviews and worked tirelessly to bring this enormous task to a successful conclusion. Without this dedicated team the project would not have been possible. We wish to acknowledge the invaluable contribution of the expert individuals and organisations from across the globe who gave of their time, experience, expertise and advice without which, this project would not have happened.

We are grateful for the honest and open way in which our international partners and stakeholders engaged with us regarding lessons learned and shared their experiences of good practices for the safety, security and service of events. Without such engagement and insight this publication would not have been completed.

We are particularly grateful to the final authors of the publication Dr. Patrick Leahy (IEMBA) and Mr Daniel Flavin (MScEM), both of whom are former senior police officers with long-established expertise in event safety/security and emergency management. They worked in partnership with the Project Stadia Team to complete the final phase of the research programme by reducing and reorganising the research data, combining it with recent international developments and transforming it into the usable information that is presented in the publication.

It is a pleasure for the INTERPOL Project Stadia Team to make this document available to our members worldwide.

DISCLAIMER

The information and key considerations consolidated within this executive summary are provided for general reference and knowledge in relation to the security aspects of major international events. The information must be adopted at the discretion of the reader, with appropriate and adequate legal advice specific to his/her jurisdiction. Certain activities such as related to international cooperation (i.e., MoU, extradition, foreign law enforcement operation within a country), border management, public and private security integration, deployment and use of video surveillance systems, use of the armed forces in support of the civil authority, use of drones, use of biometric data, if sought to be undertaken, may include the need for specific procedural steps to be taken, or a legal basis under applicable laws. In case of any uncertainty, the reader's recourse is to consult the relevant law enforcement, legal and judicial authorities in his/her jurisdiction. INTERPOL does not and cannot provide legal advice or legal basis for undertaking any of the actions mentioned herein. INTERPOL shall not be liable for any actions taken or omitted by any reader on the basis of the contents of this executive summary, including with respect to any proposed investigation or prosecution.

The legal, procedural and customary frameworks in respect of safety and security activities in major event policing, differ widely by jurisdiction. This executive summary does not provide any recommendations, advice, or instructions in respect of requirements under such legal and procedural frameworks in any jurisdiction and any references seemingly suggesting as such should be read as being subject to domestic laws and procedures in this regard. Readers are advised, when taking any actions based on this executive summary, to verify and ensure that such actions are in compliance with appropriate legal and procedural requirements or standards in their jurisdiction. Where references to certification processes, MoU or specific arrangements, prohibited items, drone offences or use of facial recognition technology are provided, these are intended to be used as suggestions, and not to replace existing documents in use in the reader's jurisdiction and such matters are subject to consultation with the appropriate national authorities. In particular, where legal requirements exist in the reader's jurisdiction as to the content or form of such documents, it is the reader's duty to refer to those requirements in conjunction with or in replacement of those contained herein.

The content of this executive summary may not constitute a complete overview of legislative resources. Readers are advised to contact competent national authorities if they require any further information regarding the applicable legal framework and relevant requirements. In addition, this executive summary does not constitute legal or other professional advice or an opinion of any kind. This executive summary is not mandatory in nature and has no enforceability. INTERPOL shall not be liable for any actions taken by any parties based on this executive summary which is contrary to or inconsistent with or not in compliance with any relevant legal, regulatory, administrative, procedural, evidentiary, customary, or other requirements.

INTERPOL General Secretariat

200, quai Charles de Gaulle

69006 Lyon France

Telephone + 33 4 72 44 70 00

EXECUTIVE SUMMARY

INTRODUCTION

Major events such as the Olympics and FIFA World Cup, carry an inherent burden in terms of safety, security, service, integrity and legacy, but they can also have implications for a country's sovereignty, prestige and reputation, particularly should things go wrong. The hosting of a major sporting event brings with it a national responsibility on the part of the host government to safeguard the event, including protecting the participants and spectators. Major events require effective and sustainable security strategies and operational responses. In addition, these events involve enhancing public order and crime prevention, and improving the standard national security policies and practices. In the very early stages of preparation, the development of comprehensive security strategies and policies, followed by the design of a national security plan for major events, are extremely important elements that contribute to a trouble-free event.

BACKGROUND

Funded by Qatar, Project Stadia was initiated and established by INTERPOL in 2012. The aim of Project Stadia was to create a Centre of Excellence to assist INTERPOL member countries in planning and executing policing and security preparations for major international events. This 10-year project has contributed to policing and security arrangements for the 2022 FIFA World Cup in Qatar and is expected to leave a lasting legacy for the World's law enforcement community.

A core component of Project Stadia has been to examine existing and emerging knowledge by organising expert group meetings on the key thematic areas of legislation, security and cybersecurity. These meetings brought together global experts from law enforcement, event organising committees, government, the private sector, academia and civil society to explore state-of-the-art research and analysis and develop independent recommendations for planning and executing security arrangements for major international events. Project Stadia then consolidated the research and recommendations into their relevant areas of security in this single publication so that it could be taken into consideration by law enforcement personnel, tasked with event security management. The information accrued has been cascaded into the following ten (10) integrated, interrelated and interdependent thematic areas that combine to represent the safety, security and service landscape for major events and those responsible for their safe and secure implementation. Each thematic area has been presented as a chapter with associated conclusions and key considerations which are outlined hereunder with a view to presenting the reader with a comprehensive overview of the content and key points.

1. New or Amended Legislation
2. Planning and Preparedness
3. Traditional and Cybersecurity
4. Technology and Biometric Data
5. Interoperability and International Police Cooperation
6. Communications
7. Crowd Management
8. Risk-Based Resource Allocation
9. Exercising and Testing
10. Emerging Challenges

1. NEW OR AMENDED LEGISLATION

The complexity of the major event industry and environment, which often includes a mix of local, national and international venues and stakeholders, requiring a balance between central coordination and decentralised implementation, is often addressed by host country guarantees and agreements facilitated by the introduction of new or amended legislation and regulations. The pre-event assessment of legislative needs however, and the subsequent development and effective application of new or amended legislation is a long-term strategic process requiring a lead-in time of several years. Therefore, the role of government is crucial in not only ensuring that a comprehensive legislative and regulatory framework is in place, but that it includes operating arrangements that oblige agencies with clear legal primacy to consult with partner agencies regarding matters that may impact on their respective operations. Optimum outcomes are best achieved through multi-stakeholder cooperation and coordination and the adoption of a comprehensive risk assessment culture designed to identify the measures necessary to provide a safe, secure and service-oriented event. In this context, significant international, national and local cooperation, collaboration and coordination needs to be supported by appropriate legislation, regulation and agreements.

Key Considerations

- The host country national co-ordination group should comprise of personnel that have the authority and capacity to make or influence key policy decisions.
- Where new or amended legislation exists, it should define the roles and responsibilities of key stakeholders.
- Competent public authorities should put in place regulations or arrangements to guarantee the effectiveness of stadium licensing procedures, certification arrangements and safety regulations in general, and ensure their application, monitoring and enforcement.
- The ethos adopted should centre on protecting the health and well-being of individuals, in their capacity as spectators, participants or employees, focusing on the identification of all potential safety risks, implementing measures designed to eliminate or reduce those risks, and having contingency arrangements in place for dealing with any incidents or emergencies.
- Consideration should be given to how host countries can use memoranda of understanding and country-to-country agreements to support delivery of policing and security arrangements, for example, through the sharing of information/intelligence, personnel exchanges and investigative support arrangements.
- Host countries should consider the establishment of fast-track judicial courts to deal quickly with criminal activity committed during the event.
- There should be early engagement between the host and other countries to facilitate timely and effective agreements.
- Host countries should engage with previous host countries to identify effective mechanisms, good practice, and develop strong partnerships with the private sector.
- Private security companies and stewards should have strict and rigorous training and certification standards that are governed by national legislation, and Individuals undertaking designated activities within the private security industry should be individually licensed by a government authority.

- Consideration should be given to developing or amending legislation related to the use and deployment of video surveillance systems, including as appropriate, facial recognition technology (FRT). These are lawful provided there is a legal basis in the given jurisdiction.
- Consideration should be given to developing and/or amending appropriate legislation related to protests and demonstrations, which provides for engagement and dialogue with protestors/demonstrators and the safe facilitation of protests and/or demonstrations where constitutionally appropriate.
- Consideration should be given to the development and/or amendment of legislation to support policing and security efforts to mitigate the risk from drones during major events.

2. PLANNING AND PREPAREDNESS

The strategic direction for the safety and security of an event in the planning phase should be formulated some years in advance. The strategic planning principles should be developed to aid long term planning and the risk concept should be developed to define how risk assessment processes will be implemented. Planning phases should operate within timeframes where key objectives have been identified, and from a safety and security perspective detailed planning discussions should take place several years prior to the event with stakeholders considering private and public security deployments, security equipment and technology, transport, traffic management and security, contingency and emergency planning, and other issues relating to the delivery of a safe, secure and service-oriented event.

Key Considerations

- Planning from inception to the staging of the event should take place over several years. The purpose should be to identify the strategic direction for the safety, security and service-orientation of the event involving all relevant functional agencies, including government departments, local authorities, and other key stakeholders.
- Tactical planning should enable the development, testing and alignment of planning and response plans for all the agencies involved.
- Operational Planning should be aligned to the tactical and strategic planning principles ensuring coordination and communication are maintained throughout the event cycle and that any required responses are provided in a structured and coordinated manner.
- A low-profile style of policing, through facilitation and integrated mobility should assist in maintaining a safe, secure, and welcoming event. Key to success is an effective communications policy, high levels of tolerance, fast responses, an understanding of behaviours and cultures and the promotion of legitimate intentions and behaviours.
- An effective planning process should ensure that mitigating measures identified in the risk assessment are applied through the risk management process.
- INTERPOL's '*Guidance for Managing Major Event Public Health Risk*' should be used to support LEA's in identifying, analysing, evaluating and managing the risks posed by pandemics and other public health threats.
- Early planning and information to the public on the implications of any proposed changes to traffic management along with information on additional transport arrangements is critical, not

only for the crowds attending the venue, but also for the volunteers, staff, businesses and residential community in the vicinity of key terminals, stadia and fan zones.

- Adopt a 'Trust but Verify' approach to 'Planning and Preparation, Implementation, Response and Recovery', to ensure that planned safety and security mission-critical actions and activities are independently confirmed, as the planned outcomes are more important than the short-term relationships between the parties.

3. TRADITIONAL AND CYBER SECURITY

The successful security of a major sporting event is the culmination of meticulous planning, co-operation and integration of experience, knowledge and information. The building of trust among practitioners, who are dealing with issues escalating in volume and complexity as the event day approaches, is made easier with the identification of a common purpose. The adoption of a structured approach, supported by ongoing dynamic risk assessments creates an inclusive environment, which, when correctly communicated, will build resilience, trust and capability among all the participants. Other environmental factors including political and legislative frameworks must also be considered and included in the planning process.

Cybersecurity is part of the overall operational security for an event which ensures that the IT processes and systems work as per requirements and represents a mission-critical element of effective planning and preparation for safe, secure, service-oriented and successful events. In an events context, there are three key aspects of cyber risks, that is, an operational element, whereby, the core operations system of a security agency may be attacked and damaged or even rendered inoperable, a legal and litigation risk, whereby, in the aftermath of an attack, those in charge of security may be held liable by third-parties who have been affected, and reputational risk, whereby, the organisers of a major event may be reputationally damaged by failing to protect the event against cyber-attack. Host countries must ensure that cyber security for major sporting events is based on a clear understanding of cyber security risks and challenges, and therefore, the associated risks and challenges must be identified, analysed, evaluated, and effectively managed in this context in order to maintain a safe and secure environment, preserve the integrity of the event and protect the reputation of hosts and organisers.

Key Considerations

Traditional Security

- Engage in the planning process at the earliest possible opportunity.
- The threat landscape represents a changing environment and therefore the security planning and response capabilities should be sufficiently flexible to meet the emerging challenges.
- Align the organisation's event security planning with the National Risk and Threat Assessment which should include emerging terrorist and cyber threats. Shortfalls in legislation should be identified and escalated for consideration by the appropriate Government Department.
- Conduct a gap analysis to identify shortfalls in training requirements, human resources and equipment, expert skill sets, analysts, and intelligence resources.
- Vigilance from the outset among all stakeholders, reinforced with regular communication to all staff on activities and objectives, offers reassurance and focus to the operation.

- Conduct a full risk and threat assessment to identify and address all operational issues that are consummate with the scale and impact of the event for the location.
- Develop definitive roles and responsibilities which must be supported by defined Standard Operating Procedures.
- Deploy a joint operations centre (JOC) which has the capacity to improve communications and understanding of inter-agency demands and offers greater integration and utilization of information and resources.
- Information gathered, promptly shared and appropriately escalated will support the intelligence building and risk management process.
- Host countries should ensure the effectiveness of the command, control and coordination functions (by implementing audits, regular exercising and constant review/improve process).

Cybersecurity

- Cyber security should protect major events and guarantee the efficient and continuous delivery of mission-critical support activities and IT services, by reducing the risk potential to as close to zero as is possible through appropriate cyber security structures, systems, processes, resources, policy, strategy, legal framework and leadership.
- Ensure collaboration in both research and response between government, commercial and academic sectors, and gain international support early to establish trusted intelligence sharing channels, expertise, and computer emergency response (CERT & CSIRT) support.
- Host countries should consider adopting a 'trust but verify' approach when it comes to stakeholder readiness assessment.
- Cyber security itself is not the objective, it is part of the overall operational security for the event which ensures that the IT processes and systems work as requirements and fallback infrastructure and scenarios are in place and tested to ensure continuity in case of intrusion or disaster.
- Consider starting with a dedicated team that acknowledges and accepts that cyber threats ignore borders, speed of response is essential, other stakeholders must be identified and involved, and a CSIRT community must be created and enabled.
- Consider separating networks, making optimum use of the cloud and other key IT stakeholders (avoiding Intra-Networking as much as possible), beware of interconnectivity through the IoT (Internet of Things) and always ensure at least 'Two Factor Authentication' (2FA) for important assets.
- Engage in Integrated Security Management – Intelligence-Driven Security.
- Cyber crisis management should be an integral part of the Business Continuity Programme and the Disaster Recovery Plan, integrated into the overall crisis management approach, supported by scenario planning and exercising.
- The senior executive team in charge of organising a major event, including stakeholders, need to be prepared to deal with cyberattacks and to understand cyber security challenges.
- Cyber security legislation should aim to facilitate the monitoring, detection, prevention, mitigation, prosecution and/or management of incidents.
- Host countries should ensure the effectiveness of the command, control and coordination functions (by implementing audits, regular exercising and constant review/improve process).

- Cyber security should not be perceived as an issue related to technology alone, but one where human behaviour is equally important. Therefore, 'cyber-hygiene', that is, routine measures implemented regularly by individuals, will minimise their exposure to risks from cyber threats, including cross-border incidents.

4. TECHNOLOGY AND BIOMETRIC DATA

Despite the potential benefits of using technology and biometric data for policing and security associated with major events, there have been clear international concerns. For example, the European Parliament cautions that digital technologies in general and the proliferation of data processing and analytics enabled by artificial intelligence (AI) in particular, bring with them extraordinary promises and risks. The right to data protection is also particularly relevant in the field of security in major sporting events, as many new technologies or special investigative techniques have considerably increased law enforcement capabilities to gather and store data. In this context, host authorities should comply with applicable regulations and standards, such as the Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, also known as Convention 108, which is the sole international treaty on data protection (open to accession to any country in the world with a complying legislation). The challenge demands a tailored approach to the design, procurement and management of surveillance technologies that appropriately blends policy, political and human rights considerations with more traditional technology management practices. In this context host nations must ensure that they have in place, effective safeguards to exploit the benefits of current and emerging technologies.

Key Considerations

- Host countries should acknowledge that increasingly, biometric data is considered especially sensitive and consider processing it only where there is a "substantial public interest", and it is subject to strict necessity and proportionality requirements.
- Facial recognition technology facilitates accelerated access, with smaller queues and enhanced throughput, while also providing a deterrent to unauthorised access and to those intent on disruption, criminality and/or terrorism. Supported by CCTV analytics it can also link a face with clothes, colours and objects with a view to managing behaviour or suspicious activities and it can also trigger and send alarms. Host countries should ensure that the public have confidence that its use is lawful, fair, transparent and meets the standards set out in data protection legislation.
- Because of the potential negative effects of system errors or misuses in the domain of biometric data (in particular, facial recognition technology) there is a pressing need to design and implement a robust governance framework to mitigate these risks, and failure to build such a framework could have dramatic consequences.
- The international governing bodies and associations that have ownership/control of major sporting events often require government guarantees, hosting agreements and host city agreements, relating to minimum measures, duties and responsibilities which generally focus on the systems implemented to address crowd and fire related incidents, and therefore, host countries should prepare for this in advance.

- Video analysis systems as a safety and security support should be available to the police and to the venue operations centre (VOC) and should include a central server indexing all information. It should also include the latest generation full-HD 'IP' wired and wireless cameras that can be deployed at locations around a stadium or other event site and viewed from any device (including off site with the appropriate security level access and accreditation).
- Drones pose a significant threat to public safety and security if abused, therefore it is crucial that officers are equipped with the necessary knowledge and training to respond to drone incidents safely and effectively and are in a position to select the appropriate technology to detect, track and intervene when an illicit drone enters the airspace.

5. INTEROPERABILITY AND INTERNATIONAL POLICE COOPERATION

The development of a Unified Command Centre should provide a strategic level of command and connectivity between the various police services involved in a major international sporting event. It is not intended to override or supersede the decision-making authority at the municipal, regional, or provincial levels, but provides a strategic level of command and connectivity between the various police services, from which venue operations can be directed and from where the safety and well-being of all persons on site should be monitored.

Key Considerations

- Host countries should consider developing and communicating a clearly defined set of roles and responsibilities directly related to individuals and/or organisations (key stakeholders), to facilitate effective collaboration, co-production and coordination.
- Host countries should consider including the following 5 key principles in their approach to interoperability: co-location, communications, coordination, joint understanding of the risk, and a shared situational awareness.
- The sharing of stakeholder's expertise in an interoperable environment should assist in developing harmony and ensuring greater productivity with resources.
- Operating with a clearly defined and easily understood methodology should enable stakeholders to understand more easily the rationale for certain police requirements.
- To achieve the safety and security orientation of major events, host countries should ensure that policing strategies and tactics are determined through continuous risk assessments and risk-based deployment of local and international police personnel.
- If not already in place, the host country should establish and resource at national level, an 'International Police Cooperation' unit/department or other suitable structure, for example, the National Football Information Point (NFIP) system as the central point of contact and coordination for international police cooperation planning and implementation.
- The security planning system should bring together multiple agencies with diverse backgrounds. Their ongoing engagement at various levels as executive leaders, senior leaders, mid- level managers and tactical planners has been identified as being key to the success of a major international event.
- The International Police Cooperation Centre (IPCC) significantly enhances the level and speed of information exchange, serving as a hub for international police cooperation. It provides

transparency for the international community, offers tailored support to international visitors and acts to prevent criminality and public disorder at major sporting and other events.

6. COMMUNICATIONS

Communications must be appropriate, capable of accurate interpretation and provide the intended information, however, the challenge to achieving this is likely to be escalated for a major international event or in times of emergencies and crisis when audiences require information that may have significant or life changing consequences for them. Audiences will first go to their trusted sources of information, and therefore, this trusted source must provide clear, continuous and reliable information. If these criteria are met, audiences are liable to remain with this source and revisit this source frequently in a crisis. Carefully resourcing, training and deploying a communications team enables an organization to respond appropriately and progressively. Pre-planned, stakeholder-agreed messaging for intended audiences should be informed by a consideration of intended and potential unintended consequences arising from the content, method of delivery, scope, accuracy and truthfulness of communications, and these elements should be addressed in the communication planning process. A proactive communications strategy through the press, social media and directly to the public can assist in providing assurances to the public and to stakeholders, that venue locations are safe and secure.

Key Considerations

- Host countries should consider that cultural differences and influences between individuals and societies may result in information being received and interpreted in different ways, potentially resulting in a variety of outcomes and unintended consequences.
- To enable a flow of information to and from stakeholders it is important to understand the needs of stakeholders, whether they are internal or external to the organization, and what the communication is intended to achieve.
- A support network may be required around the communication process, which includes skilled design of the message, its delivery, promptness and evaluation.
- Host countries should be capable of raising awareness of the indicators of terrorism and the importance of reporting suspicious activity through outreach efforts and partnerships.
- Host countries should take all reasonable steps to adopt an integrated multi-agency approach to safety, security and service, in recognition that consultation and communication with key stakeholders, including supporters and local communities, can assist the relevant agencies in reducing the risks to safety and security and in creating a welcoming atmosphere inside and outside of stadiums and other event locations.

7. CROWD MANAGEMENT

One of the principal roles of the police in connection with major sporting and other events centres on crowd management and on preventing and responding to public disorder and criminality in public and private spaces. Police match commanders, emergency controllers, intelligence officers, spotters and uniformed operational units must all effectively deliver on their important roles in meeting these objectives. In this context, they must have an understanding of the routes available for crowd

movement, with a view to conducting crowd risk analysis, including normal and emergency flow rates at ingress and egress points while adopting an integrated, interrelated and interdependent all-hazards approach. This approach must operate in continuous cycles of contextual understanding, risk identification, analysis, evaluation and mitigation evolving in parallel with the development and implementation of the event management plan, security, crowd management and emergency response plans.

Key Considerations

- Host Countries should be aware of three common failure categories associated with crowd-related accidents and incidents, that is, design, information and management. This facilitates effective risk management through the subsequent formulation of crowd management plans that systematically progress through the three primary phases of crowd movement (ingress, circulation and egress) while addressing the influences on crowd behaviour at each phase.
- Effective crowd management is essential, and this requires competent crowd safety professionals who know the venue and understand its associated nuances as it moves from event to event.
- Evacuation plans must operate on the same end-to-end basis as the crowd management plan, that is, they must consider the three stages of movement, ingress, circulation and egress as potential risk areas where an emergency evacuation may be required.
- Estimates for the time spent at doors, gates or in corridors during an evacuation should not be based exclusively on the mean flow rate at the bottleneck under study, i.e., its capacity, as these times may fluctuate considerably, especially when the relative narrowness of the bottleneck and the competitiveness of the crowd favour highly intermittent dynamics.
- Event organisers should make provision for the development of a transportation concept including identification of stadium/event location transport perimeters and applicable guidelines.
- Host nations should consider the use of privacy-friendly/aware smart technology to enhance the overall operational security of the event and the effective and efficient management of spectators/crowds, for example, using a 'Smart Technology Identification Card' with Radio Frequency Identification (RFID), when lawful within the jurisdiction.
- Effective delivery of crowd management policing responsibilities requires a sophisticated policing strategy, incorporating risk based, graded deployment, dialogue and interaction with supporters, early and targeted intervention to prevent minor incidents escalating in scale, and robust evidence gathering arrangements for prosecution and exclusion purposes.
- Multi-agency preparations should take account of all matters that may impact on the event day dynamic, including policing strategies, stadium licensing, ticketing, stewarding and other in-stadia operating arrangements, local hospitality and related activities (including community and supporter liaison), transport and other logistical factors, and crisis planning for emergency scenarios (inside and outside of stadia).
- The nature, role, and functions of stewards should be clearly defined. If not prescribed by law, when working at an event that also includes the police there should be a written agreement which clearly identifies the distinct roles and responsibilities of both stewards and police, in normal circumstances and in the event of an emergency.

8. RISK-BASED RESOURCE ALLOCATION

Risk-based resource allocation has increased in importance across all sectors including the events industry. As societies have matured, citizens have become ever more insistent on living in safe and more predictable conditions, and the number of laws and regulations have increased, expanding the scope of necessary enforcement. In this context, regulatory and enforcement agencies face pressure to fulfil their missions with tighter and tighter budgets and establishing tolerable levels of risk has therefore become one of the most contentious and important risk management decisions.

Conceptually, risk can be considered as the intersection of events where threat, vulnerability, and consequences are all present. To combine risk management and resource allocation associated with major events, the approach must be dynamic in its application, incorporating an integrated, interrelated and interdependent risk/threat identification process. This includes continuous cycles of contextual understanding and vulnerability assessment, risk analysis, evaluation and mitigation, and an evolving risk management plan developing in parallel with the continuing development and implementation of the event management plan, security, crowd management and emergency response plans.

Key Considerations

- The output of the risk assessment process should be an input to the event planning process in terms of resource allocation and the organisers' decision-making process relating to safety, security and service at the major event.
- The major event risk management process should commence prior to the formulation of an event strategy or the start of the strategic planning process.
- The event strategy and strategic objectives must be defined, strategic risks must be identified, analysed, evaluated, treated, monitored and reviewed, and this must take place regularly, in line with changes to the strategy or strategic objectives.
- Any increase in the resourcing of major events that is above and beyond normal policing levels must be supported by accurate risk assessments and must reflect the level of risk identified.
- The approach to risk-based resource allocation should be a continuing cyclical process that reflects the strategic, operational and tactical planning processes and any changes that materially affect those plans.
- When the level of each individual risk has been determined based on risk analysis and evaluation, the treatment options, including any additional resources, human, technical and informational that are required, must be costed.
- Monitoring and reviewing the implementation of risk treatment options and activities is essential to the optimum use of scarce resources, and key stakeholders will expect that a process is in place to ensure the appropriate allocation, reallocation, and effective use of resources at all stages of a major sporting or other event.

9. EXERCISING AND TESTING

One of the key benefits of conducting exercises is that they provide a safe place to fail. They are cost effective, they improve skill and confidence, and they identify vulnerabilities, however, for optimum effect the exercise or test must be planned and aligned to the Event Management Plan. Joint planning

and exercising are critical to the success of the policing role and should be conducted to validate the operational plans and examine the overall level of preparedness. Exercising for major events should adopt a graduated approach, starting with introductory exercises such as a seminar, potentially culminating in a full-scale exercise closer to the time of the actual event.

Key Considerations

- A central element of the exercising function should be the testing and evaluation of emergency response plans.
- The event plan and risk assessment process does not convey safety-critical information in a quick and easy-to-understand format and as a consequence this should be addressed in pre-event testing, with personnel focusing on crowd movement during normal and emergency situations and walking the site to develop such understanding.
- A graduated approach to exercising should consider the following 5 stages of deepening engagement and learning, seminars, workshops, tabletop exercises, functional exercises and multi-agency coordination full-scale exercise.

10. EMERGING CHALLENGES

Major international sporting and other events will remain susceptible to attack or interference due to the public nature of the product/service they deliver which is dependent upon advertising (through effective marketing), at global, international and/or national level. Sponsors, who are a critical element of the financial structure that enables major international sporting events require/demand such advertising in order to recoup their financial outlay and make short term and long term profits. In this context, malicious actors such as terrorists, serious and organised criminal networks, cyber-crime actors, hooligans, protestors and others who identify such events as platforms for their respective interference/attack have ample time to prepare and execute their actions/activities deep under the radar or in a media environment where their actions will be live streamed across the globe.

Whatever their motives or methods however, major international events represent a target-rich environment for those who are so inclined. Motivations and methods of malicious actors do not remain static however, and therefore the major events industry must be agile and flexible in its planning and implementation of events (underpinned by effective interoperability) and also in its capacity to change and address emerging challenges. This requires leadership, policy and strategy, people, partnerships, resources and effective processes at an international level, supported by effective legislation, intelligence sharing and borderless cyber security cooperation.

In addition, governments and the major events industry must consider the broad effects of climate change and its influence on weather and other natural disasters which indicate that the major international event industry must throw the net wide when considering emerging threats. It must also consider emerging crime trends and related criminality and develop an understanding that effectively countering crime will require commitment from and close collaboration with all member countries, regional police organisations and other critical public and private sector partners working collectively

with INTERPOL in coalitions against transnational criminality.[1] It is also suggested that operational cooperation must be prioritized at the national, regional and global levels and the timely sharing of information between public authorities and private sector actors must be increased.[2]

Key Considerations

- Key actors associated with the major event industry, including national governments/hosts, international associations/bodies and other key stakeholders must continually engage in environmental scanning and expand their horizon to identify and understand emerging risks and challenges which would not have been considered as traditional areas of concern.

- Recent occurrences at major international sporting and other events, indicates that effective stakeholder interoperability is not being achieved and therefore represents an emerging challenge in the context of planning and preparedness, but more importantly, implementing and responding effectively in the live environment. Research suggests that individual teams tend to focus on agency-specific behaviour, as opposed to coordinated multi-team functioning, and so collective interoperability is not being achieved. It is suggested that this reduces the ability to perform collaborative behaviours, including decision-making and action implementation.

CONCLUSION

This report clearly indicates that planning and implementing a major event is challenging and is not a linear process. It requires the effective integration of multiple plans and activities within the overarching framework of a strategic plan developed, maintained and actioned at international, national and local levels. This is necessary to facilitate a cooperative and collaborative approach between a diversity of key stakeholders who are required to work together in order to deliver safety, security and a service oriented, welcoming environment and experience. To achieve this outcome, effective legislation must be in place; long-term planning and preparedness must be appropriately managed; traditional and cybersecurity must be combined under one security umbrella; appropriate technology and biometrics must be explored and engaged; interoperability at national and international level must be achieved; communications must be holistic and effective; the management of large crowds must use international best practice under the stewardship of experienced personnel; risk-based resource allocation must reflect the cost, and exercising and testing must take place at every level to ensure operational effectiveness under normal and emergency conditions.

In addition, it is essential that the major event industry (including public and private sector stakeholders) engage in continuous environmental research to identify global, international and national political, economic, societal, technological, legal, environmental/climate and criminal trends so that emerging challenges can be identified and taken into consideration when deciding to award hosting rights for major events. The industry could equally explore opportunities to champion some of the more societal, economic and environmental/climate elements that have the potential to influence all other issues and challenges.

---

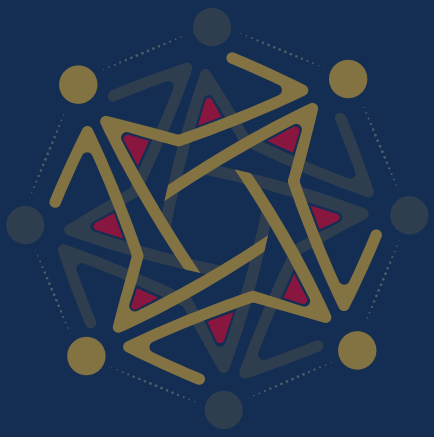
[1]. INTERPOL. *INTERPOL Global Crime Trend Summary Report*, *Key Findings*. Lyon: INTERPOL, 2022, 10. Accessed 3rd November 2022. https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

[2]. Ibid, 10.

INTERPOL has published numerous guidelines, SOP's, and other guiding materials over the years that can be additional valuable resources for those involved in major event planning, security, and response efforts. Interested parties are encouraged to contact INTERPOL for further details.

It must be noted that this document is merely an executive summary and should be treated accordingly. The main document upon which this summary is based contains significant important safety, security and service detail which is not available in this summary.

INTERPOL



www.interpol.int

INTERPOL

@INTERPOL_HQ

INTERPOL_HQ

INTERPOL HQ

INTERPOL