

Growing Terrorism Challenge for Sports Events

The issue of security at high-profile stadiums and major sporting events has gained considerable attention in the wake of the 13 November 2015 terrorist attacks in Paris. The incident saw the Stade de France, the iconic national stadium situated in Saint-Denis, north of central Paris, targeted during a series of coordinated assaults carried out by seven terrorists linked to Islamic State (IS) in the most significant terrorist event in France's history. With France hosting the football European Championships from 10 June-10 July 2016, and Rio de Janeiro the Olympics Games in August 2016, to name but two events, security agencies are now tasked with the increasingly complex challenge of protecting global sporting events from mass terrorist attacks.

Key Observations

- Improved stadium design and security will continue to inhibit attackers from gaining access to stadiums. However, event organisers will need to remain aware of the evolving terrorism threat and ensure mitigating strategies are in place.
- Continued assessment and improvement of stadiums' physical security, procedures and crowd control measures will increase financial and logistical challenges for event planners and organisers.
- Heightened security at high-profile sporting events will become standard procedure.
- Paradoxically, increased stadium security will present attractive terrorist targets as potential target locations expand into areas around the stadium where large crowds gather, particularly on approach routes and at nearby transport hubs.
- Corporations and individuals attending high-profile sporting events will need to be more conscious of their own security due to the additional pressures upon public resources, taking into consideration incident management and emergency response planning.

Motivations

Sport is no stranger to the threat from terrorism. High-profile sporting events, including the Olympics, football tournaments and cricket matches, have been targeted, with varying degrees of impact and success since the 1972 Olympics in Munich, Germany. A number of incidents have been prevented at high-profile sporting events in recent years due to successful counter-terrorism operations.

The assault on the Stade de France in November 2015 illustrates the increasing threat from Islamist-related terrorism, especially IS-affiliated entities or sympathisers. Football tournaments are highly attractive targets, with non-Muslim and Muslim supporters and players alike creating a multicultural environment. This cultural and religious diversity is a key motivating factor for IS and such attacks are anticipated to continue. Furthermore, the media attention generated by sporting events is another driver. IS is critically aware of its propaganda campaign and the manipulation of social and mainstream media to increase its profile. As such, the combination of the growing threat from IS, the media attention garnered by the group and sporting events, as well as the presence of a large, condensed crowd of people in a restricted area, makes sport a prominent terrorism target. This is underpinned by what sport is deemed to represent – togetherness, integrity, inclusivity, among other values that IS, and other groups, diametrically oppose.

Successful attacks

- 1996 - Centennial Olympic Park, Atlanta, US; bombing leaves one dead and 111 injured
- 2002 – Karachi; Pakistan; New Zealand cricket team hotel targeted leaves 14 dead including nine French nationals
- 2009 – Lahore, Pakistan; Sri Lankan cricket team deliberately targeted by Lashkar-e-Jhangvi militants, killing six officers and injuring several team members
- 2013 – Boston Marathon, US; two bombs detonated near the finish line leave three people dead and more than 260 injured

Foiled plots

- 1998 – FIFA World Cup, France; Police arrest 100 people in several countries over plan targeting the Marseille stadium to kidnap players and officials in the England vs Tunisia fixture, as well as the hotel used by the US team
- 2000 – Euro 2000, Belgium/Netherlands;
- 2004 – Euro 2004, Portugal; police arrest three Islamists planning to target former Portuguese Prime Minister Jose Manuel Barroso
- November 2015 - Germany-Netherlands football match, Hanover; bomb threat led to the evacuation of the stadium

Case Study: Stade de France Attack

The impact of the attack at the Stade de France stadium on 13 November 2015 appears to have been limited by security measures at the stadium. The first suicide bomber was frisked and discovered by a security guard at Gate J, before stepping back and detonating his device, killing himself and a bystander. The incident took place some 15 minutes into the match at around 2120hrs local time. Around three minutes later, a second person also blew himself up outside the stadium near Gate H. A third suicide attacker detonated explosives at a nearby McDonald's restaurant. The explosions were heard inside the stadium, but it appears many in attendance assumed the noise was made by fireworks, common at European football matches.



Initial assessments suggested the bombers wanted to enter the stadium, potentially to target President Francois Hollande, who was at the match between France and Germany. Any detonation inside the stadium would have caused major panic. However, it is also possible that the bombers mis-timed their attacks, and knowing they would be unable to circumvent stadium security, intended instead to target crowds as they arrived or left the stadium. Had they managed to enter the venue, the impact would have been significant. The decision by officials to keep the crowd inside the stadium after the first two bombings as an invacuation measure almost certainly prevented casualties.

Security is now being reviewed ahead of the Euro 2016 football tournament in 10 cities across France. For the tournament, Euro 2016 SAS, a joint venture between the FFF and UEFA, will be responsible for all operational aspects of the tournament. Jacques Lambert, the chairman of Euro 2016 SAS, says he expects stadium security to be robust, but that the risk is higher on the streets and at other spontaneous gatherings. At present, the government is responsible for assuring security around stadium locations and the fan zones where matches can be watched on giant screens. Private security firms are in charge of safety inside stadiums and the French police are responsible for security outside, though law enforcement agencies as the executive authority can enter venues when required. The plans are now to be reviewed before finalisation due to threat posed by IS, with the current procedures likely to be amended for the Euro 2016.

The threat against sporting events from IS and other Islamist militant groups is set to remain a long-term concern. The 12th edition of Inspire, the al-Qaeda propaganda publication, released in March 2014, called for bomb attacks against sporting events including the US tennis open, the UK FA Cup, the English Premier Football League and the League Cup in France. Al-Qaeda in the Arabian Peninsula (AQAP), which produces the publication, also provided advice on how to carry out attacks, suggesting the best time to target a UK football match is when the crowds are leaving the stadium. IS has also threatened to target future sporting events, as well as France in general, suggesting the 2016 European Championships is a likely target. While the causal link between extremist publications and actual attacks is questionable, it would be irresponsible to ignore the impact of such calls. The Tsarnaev bombers who targeted the Boston Marathon in 2013 used guidance from the first edition of Inspire to carry out their attacks.

The threat posed by IS and its intent to target Western interests suggests the risk to sporting events is now more significant than in previous decades. IS claimed after the 13 November attacks that France would remain a priority target, along with other Western countries involved in the anti-IS coalition conducting airstrikes in Iraq and Syria. Western Europe, including France and the UK, has reported an increasing number of foiled terrorist attacks since IS declared its so-called caliphate in June 2014. As such, securing sports events, particularly high-profile games such as the Olympics, the European Championships, Wimbledon and the French Open, has become more challenging and a long-term issue.

Impact of Paris terrorist attack

The 13 November attacks on the Stade de France triggered a major response by sports organisers. In the following weeks, events across France were postponed, including football league matches and European rugby fixtures. For the Six Nations Rugby Championship match at Stade de France on 6 February, French Rugby Federation (FRF) officials implemented the largest security operation ever seen at a sports event in the country. A robust search regime was introduced, involving some 250 police officers and 900 security staff – almost double the number from previous years. Specialist teams using dogs and snipers were also deployed. The security perimeter was extended to 100m away from the stadium, with attendees searched at least twice before being allowed to enter. Public transport and routes to the stadium were also under heavy surveillance. Attendees were asked to arrive early, with the stadium opening two hours before kick-off to minimise congestion.

The threat has also been felt beyond Europe, with the security operation for the Super Bowl 50 on 7 February in San Francisco involving 4,000 personnel. Counter-terrorism planning for the event had taken three years to formalise, but was reviewed in light of the Paris attacks. Moreover, organisers of football matches in Australia have also committed to improving security in 2016 following advice and consultation with French officials after the 13 November attacks. Sporting events organisers/security managers in Japan, Spain and Trinidad also escalated security.

Attention is turning to the Summer Olympic and Paralympic Games in Rio de Janeiro, Brazil, in August and September 2016, with the current security budget estimated at some USD 195 million, significantly less than other previous games; London in 2012 (USD 870 million), Athens in 2004 (USD 1.2 billion), Vancouver in 2010 (USD 1 billion) and Sochi, in 2014 (USD 3 billion). It is almost certain that the figure of USD 195 million will have to increase substantially to effectively tackle the terrorism threat, particularly in light of the availability of firearms and high levels of violent crime in Brazil, which places additional pressure on police and other security providers. While Brazil is not considered to be a main target for Islamist terrorism, IS recruiter and French jihadist Maxime Hauchard warned on 16 November 2015 that Rio “would be next”. Terrorism will seek to follow the crowds, along with the media, as IS in particular is very media-savvy, and with the proliferation of firearms, an attack against the 2016 Rio Olympics cannot be discounted.

Terrorism Evolution and Sport

So-called “Lo-fi” attacks that involve the use of bladed weapons, tools, and even vehicles, as well as single active shooters, improvised explosive device (IED) attacks in various forms, or a coordinated attack as seen in Paris involving multiple gunmen, are considered the most likely form of terrorism against a sporting event. While it is conceivable that a single active shooter or “lone wolf” attacker could gain access to a stadium, the escalation in physical security and personnel will make this ever more difficult.

Attention is also turning to more sophisticated methods. The organisers of the Super Bowl 50 in San Francisco were warned by the FBI and Department of Homeland Security that “high-tech” issues were present and could pose a risk to the event. According to FBI sources, some 10 cables damaged within a 60km-radius of the 49ers' stadium in mid-2015. Officials believe the incidents were trial runs to see if cutting the cables would disrupt critical services or if the networks could be accessed for information regarding the Super Bowl. Damaging the cables could also hinder response times of the emergency services in the event of an attack. It is anticipated that high-tech threats surrounding cyber-terrorism will continue to be a key concern for sporting events, with the London, Beijing and Sochi Olympics linked to a heightened risk of cyber-attacks.

Additionally, the FBI warning also gives credence to the future of drones or unmanned aerial vehicles posing a possible threat to sporting events, as demonstrated during the Serbia vs Albania football match in October 2014 when the game was halted after a drone entered the playing area. Ahead of the Super Bowl 50, officials warned that drones could be used to carry out terrorist attacks involving light, explosive payloads, while the more rudimentary risk of deliberately crashing the drone inside the stadium to injure people or disrupt the event was also highlighted. The use of “high-tech” methods, whether drones or cyber-terrorism, is more likely to be used in conjunction with more traditional forms of terrorism; cyber-attacks hampering emergency services and disrupting critical infrastructure, while a deliberately crashed drone could trigger panic and disorder exposing the event to secondary and tertiary attacks involving firearms, explosives or bladed weapons.

Ramifications for events

The ramifications for sports event organisers will be significant in response to the Stade de France attacks. Event organisers will have to commit to long-term heightened security as seen during the ongoing Six Nations Rugby Championships. While terrorist organisations have targeted sporting events since the 1970s, the IS attacks in Paris and the perceived long-term threat from the group means that the sports industry will have to consider the threat and associated escalated security as the norm. Joan Carles Molinero, the commander of the Catalan police which deals with security at Barcelona's Nou Camp stadium, says security alerts are "common situations" and that the larger sporting venues may have to adopt airport-style security on a permanent basis. Measures being considered and implemented at other venues include metal detectors, pat-down searches and scanners.



Major sporting events, such as the Olympics, Commonwealth Games and football and cricket tournaments, are familiar with implementing robust security to the point where millions, or billions as in the case of the 2004 Athens Olympics and the 2014 Sochi Olympics, of dollars are spent to secure the event. However, it may now be the case that less prestigious sporting events may have to implement much tighter security, at a cost, due to the terrorism threat.

While larger, more popular venues could implement such measures, smaller venues may struggle to maintain elevated security for long periods, increasing financial pressures. Regardless of the magnitude of the sporting event, higher security costs, logistical issues and crowd control, particularly measures to manage congestion, will become key factors for organisers necessitating much closer relations with the police and public security agencies, with further financial resources likely in terms of private security personnel and stadium stewards. Additional pressures on public security resources in tackling the wider terrorism threat will likely mean that event organisers become more reliant upon private security providers. This will increase pressure on private security in terms of vetting and screening when employing security personnel. There are already concerns that poor or rushed vetting could allow vulnerabilities to be exposed, even to the point where terrorist sympathisers apply for stadium security roles with the intention of carrying out an attack once inside. Other internal stadium functions, including hospitality, catering and stewarding, which could be voluntary at some venues, would also need to be reassessed in terms of recruitment, vetting, screening, and most crucially, training. Internal staff will also have to undergo the same search regimes as spectators to ensure the stadium's security integrity. These factors will add financial pressures to security providers and organisers.

Increasing physical security is an obvious necessity to protect the venue and mitigate the threat. However, the nature of physical security means that the threat is often displaced rather than removed. There is the potential, due to the escalation in security, that crowds attending sporting events become the next most attractive target, before they enter or when they leave the heavily-protected stadium and enhanced perimeter security. Routes to and from the venue, transport hubs associated with sporting events, bars, cafes and restaurants close to the stadium could be at greater risk despite the measures undertaken, as demonstrated in Uganda and Nigeria where bars and fan-zone screenings were targeted during the World Cups in 2010 and 2014, respectively. This will place greater emphasis on liaison between stadium management and police, and with public agencies responsible for security outside of the stadium.

Crowd management

Crowd management and how to manage the ingress and egress of thousands of people within a relatively short time frame will continue to be a critical aspect of stadium security. While spectators are likely to be safe inside grounds, managing crowds

outside of a heavily-secured venue becomes more of a challenge. Robust crowd management strategies and procedures will need to be developed to ensure spectators are not exposed to greater risk while exiting or accessing the stadium.

Understanding the nuances of crowd management will become essential, with greater emphasis on managing the flow of people outside of the stadium. Core factors that need consideration are the nature of the event, the environment (type of venue, climatic conditions, route layout), demographics of the crowd and the overall mood of the occasion, including spectator grievances with organisers, teams or club representatives. Environmental factors, particularly the terrain around the venue, will have an impact on crowd management. In the event of an emergency, stadium authorities will likely use one of five fundamental crowd-related responses; total evacuation, phased evacuation, directed evacuation, stay/shelter in place and invacuation. However, these responses will need reviewing in light of the evolving threat and the direct targeting of people outside the stadium before or after the event. A closer examination of the manner in which spectators enter and exit the venue, particularly when movement is dictated by street geography, may necessitate a change in stadium procedures, policies and how crowd-related responses are implemented.



Routes used to access the stadium may experience congestion due to road narrowing, street design and layout making managing high volumes of people more difficult. Crowd congestion close to the stadium makes spectators attractive targets, particularly for “lone wolf” attackers, which present a major security challenge. One technique is road closures using soft Hostile Vehicle Mitigation (HVM) tactics; usually, the deployment of emergency vehicles to create a temporary physical barrier. This lessens the need for hard HVM, such as fixed bollards, concrete flower beds, and permanent barriers, which may not be appropriate. However, soft HVM, while a good compromise, can still cause knock-on congestion in the nearby vicinity, potentially creating more disruption and presenting secondary targets near the stadium, including emergency service vehicles acting

as soft HVM.

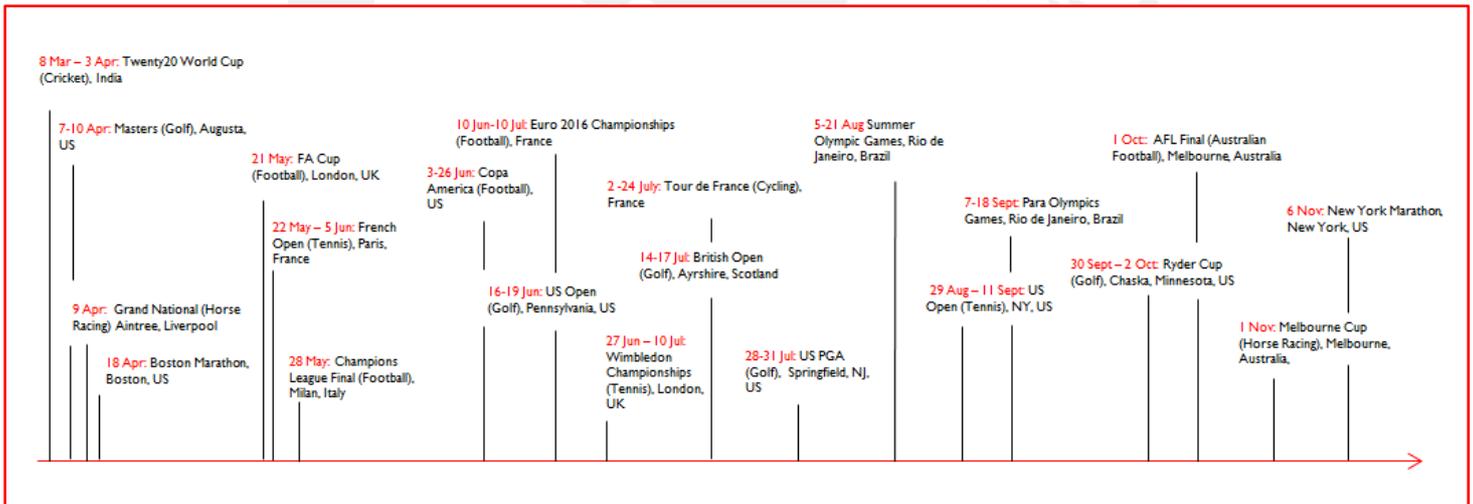
Event organisers may have to accept additional costs and entice and encourage spectators to enter the stadium earlier and stay longer, offering additional entertainment and facilities thus reducing the volume of pedestrian traffic immediately before and after the event. While this is done at major events or at times of heightened risk, extending stadium opening times and allowing spectators in the stadium for a longer period of time could become normal procedure, necessitating a review of stadium resources.

Mitigation measures

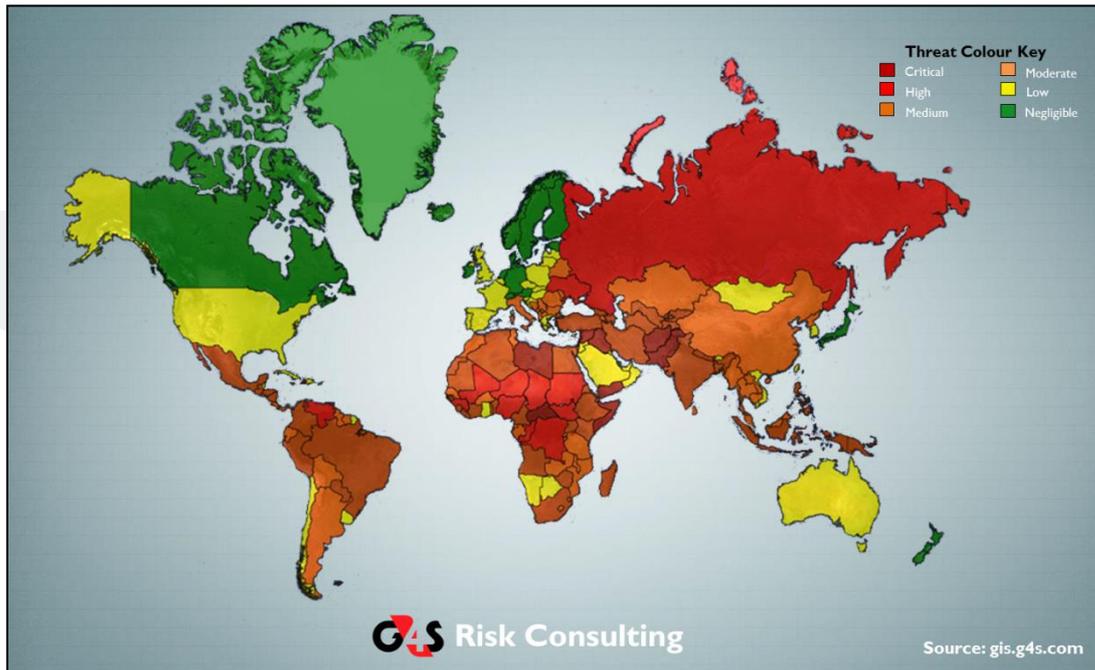
Heightened stadium security, as witnessed during the Six Nations Championships, while difficult to maintain and expensive, is anticipated to become the default position to protect major sporting events. However, the “ring of steel” approach, while effective for the stadium, presents vulnerabilities elsewhere. The next logical step is likely to be increasing security at nearby locations, including amenities, stores and transport hubs. As security is increased, the focus will shift more towards crowd management. Particular emphasis will need to be given to the dynamics of crowd control and how to manage the flow of people. Congestion, bottlenecks or impeded pedestrian as attractive “soft” targets, causing mass panic and significant casualties in the event of an attack, will need to be avoided. While protecting a flow of spectators at all times is almost impossible, using techniques such as “soft” HVM, partial road closures and diversionary measures can reduce some of the risk. Furthermore, organisers may need to consider policies concerning stadium access and egress, with staggered exit and entry used as a potential mitigation measure to limit large volumes of people assembling before or after events.

Resourcing

The difficulty in balancing public resources in terms of sustainability, cost and manpower while mitigating the terrorism threat in relation to sporting events is expected to remain a long-term issue. Finite resources may mean that heightened security witnessed at the Stade de France on 6 February may only be applicable for high-profile events, such as the European Championships or the Olympics. Private security providers may become required in the longer term to not only provide stadium security, as is often the case currently, but to also extend their role to outside of the venue, which traditionally falls within the remit of public security agencies. The additional strain on resources to protect crowds during sporting events could mean that event organisers and potentially even attendees shoulder more responsibility. Corporate guests and personnel attending high-profile sporting events may need to consider their own personal security more carefully, and have a greater understanding of their own risk management and emergency response plans in the event of a terrorist incident.



Timeline of major sports events in 2016



G4S Risk Consulting

- [G4S Risk Consulting](#) has an extensive portfolio of services across a wide range of industries and sectors. We pride ourselves on having a wealth of experience and expertise among our consultant team.
- Our core service portfolio consists of security risk management; risk analysis; compliance & investigations; training & capacity building; cyber and digital risk.
- We have recently expanded our service lines to also offer travel risk management; remote site support services; CBRN risk advisory; fraud & investigations and we continue to build upon our offering by growing our expert team of consultants.
- The [Global Intelligence System](#) (GIS) is an online monitoring system providing geopolitical intelligence on current and future threats to corporate security, travel and business continuity. GIS uses a quantitative risk rating model and qualitative analysis to assess the threat level in 220 countries and territories.

LEGAL DISCLAIMER

This report has been prepared by G4S Risk Consulting Limited ("G4S") for information purposes only, and is in no way intended as a substitute for tailored advice separately requested from G4S.

THIS REPORT DOES NOT CONSTITUTE A RECOMMENDATION, ENDORSEMENT, OPINION OR APPROVAL OF ANY KIND WITH RESPECT TO ANY TRANSACTION, DECISION OR EVALUATION, AND SHOULD NOT BE RELIED UPON AS SUCH UNDER ANY CIRCUMSTANCES.

Any reliance on or use of this report by a recipient, in whole or in part, shall constitute deemed acceptance of this legal disclaimer. G4S warrant that they have prepared this report using reasonable care and skill and in accordance with generally recognised commercial practices and standards. G4S assumes no liability, whether direct or indirect, to any person who is not the intended addressee or intended recipient of this report, for the information contained herein, its interpretation or applications, or for omissions, or for reliance by any such person thereon. To the extent that either G4S incur liability for this report, they shall not be liable to any person, whether in contract, tort (including negligence), for breach of statutory duty, or otherwise, arising under or in connection with this report for any indirect or consequential loss suffered by any such person. To the extent that information provided in this report is based on a review of publicly-available records or confidential independent third party sources, G4S shall use its reasonable and commercial endeavours to verify the truth and accuracy of such information which may be dependent upon the time and/or resource that G4S have available to them. Statements herein concerning financial, regulatory or legal matters should be understood to be general observations based solely on G4S experience as consultants and may not be relied upon as financial, regulatory or legal advice, which G4S is not authorised to provide. All such matters should be reviewed with appropriately qualified advisors in these areas.

All rights in this report are reserved by G4S and there shall be no express or implied assignment, grant of any licence or right to sub-licence any of the intellectual property rights set out herein to any of their recipients. G4S do not grant recipients of this report any express or implied right to copy or reproduce this report in any form.

© G4S Risk Consulting Ltd. 2016