Play it safe

New threats challenge event security

The Paris and Brussels attacks and the Orlando nightclub shooting demonstrated the vulnerability of crowds in enclosed spaces. Anthony Brooks and Shaun Romeril analyse the evolution of event security techniques, learning from the London 2012 Olympics.

Key points

- Event security is in the spotlight in 2016, with Brazilian preparations for the Olympics seeking to counter a diverse range of threats.
- Techniques deployed to assure event security typically involve advanced intelligence-gathering, physical screening, and remote surveillance.
- Future innovations will include greater use of facial recognition technology and social media sentiment analysis, deployed to deal with a range of threats, from public disorder to the increasing threat posed by lone-actor terrorists.

The Euro 2016 football tournament held in France between 10 June and 10 July faced a terrorist threat "more acute than for any international sporting event in history". That assessment, which appeared in a report published by the Combating Terrorism Center (CTC) of the United States Military Academy on 6 June, underlined the importance of the event security preparations ahead of the tournament. The Union of European Football Associations (UEFA) estimated that 2.5 million people would visit stadiums during the course of the event.

The threat was underscored by the killing of two police officers on 13 June, three days after the tournament had opened, by 25-year-old Larossi Abballa, in an attack claimed by the Islamic State. In a live-streamed video of his attack, Abballa vowed that Euro 2016 would turn into "a cemetery". His prediction did not come to pass as the tournament ended without any further terrorist incidents, although this proved to be a short-lived relief for the French security authorities. The challenges of event security were again sharply highlighted by the terrorist atrocity in Nice on 14 July, when 85 people celebrating Bastille Day were killed by Mohamed Lahouaiej-Bouhle driving a 19-tonne truck into crowds.

Although the threat of Islamist terrorism at the Olympics is lower than in France, the globalisation of terrorism and the high-profile nature of the Olympic Games nevertheless make them an obvious target. Moreover, by early July, with street robberies at an 11-year peak, concerns about a deteriorating public

The Olympic Park for the 2016 games in Rio de Janeiro, Brazil. In the run up to the Olympics, the Games and the city were overshadowed by security threats, violence, the Zika virus, and a national political corruption scandal. PA: 1647365 security situation in Rio de Janeiro had led troops to begin early patrolling of Olympic venues, with Rio mayor Eduardo Paes criticising state security preparations as "terrible".

Euro 2016 and the Olympics

After the Paris attacks of 2015, security at Euro 2016 was increased to take into account the possibility of terrorist attacks on the tournament. Patrick Calvar, head of France's General Directorate for Internal Security (Direction Générale de la Sécurité Intérieure: DGSI), told the parliamentary defence committee in May 2016 that although "the attacks of last November were carried out by suicide bombers and Kalashnikov-wielding gunmen to maximise the number of victims", the risk facing Euro 2016 was of "a new form of attack... characterised by placing explosive devices in places where there are large crowds and repeating this type of action to create a climate of maximum panic".

In the aftermath of the Paris attacks, security services have had to take into account the changing threat environment that they face from individuals and groups willing to attack high-profile sites with the intention of causing large numbers of casualties. Improvised explosive devices (IEDs), vehicle-borne improvised explosive devices (VBIEDs), suicide vests, small-arms, and grenades have all been used by Islamist terrorists against Western targets since 2004.

The activities of Al-Qaeda, the Islamic State, and other Middle East-based terrorist groups have increased the global terrorist threat posed by self-radicalised individuals and groups, as well as from fighters who have returned from conflict zones such as Syria, Iraq, and Libya. According to a study published on 1 April 2016 by The Hague-based International Centre for Counter-Terrorism (ICCT), almost 30% of the 4,000 Europeans who had gone to fight with armed groups in Syria had returned to Europe. Returnees pose a particular challenge, as limited resources mean that security services have to prioritise those considered to present the greatest risk.

The non-linear evolution in terrorist acts since the 11 September 2001 attacks on the United States has caused a change in tactics, driven by the high media interest generated by mass-casualty attacks. From the 11 March 2004 Madrid train bombings and the 7 July 2005 London bombings to the Paris attacks of 2015, terrorists have adapted their methods to stay ahead of security services, demonstrating that more 'spectacular' objectives generate more comprehensive media coverage.

PA: 1647362

French riot police confront English football fans in downtown Marseille on 11 June 2016. Fighting between supporters broke out in advance of England's first match against Russia on 11 June.

Euro 2016 was undoubtedly an aspirant target for Islamist terrorists. Mohamed Abrini, a member of the cell that carried out the Brussels and Paris attacks, told interrogators in early April that the group's original target had been Euro 2016, and the Belgian prosecutor's office declared after the arrest of key Paris attack suspect Salah Abdeslam that the terrorists had changed their plans and decided "to strike in Brussels".

At Euro 2016, French security services also faced the additional challenge of football hooliganism. Although violence between supporters of opposing teams has declined since the 1970s, it remains a problem. Innovations to reduce in-stadium violence include segregated, all-seater venues that reduce the ability of fans to move around freely; security checks on entry to enable stewards to confiscate alcohol and potential missiles; and banning known troublemakers from attending matches.

However, outbreaks of violence outside stadiums have always been more difficult to control, as shown by the repeated clashes between English and Russian fans in Marseille on 10 June 2016. Moreover, the England-Russia match also demonstrated a breakdown in stadium security as Russian fans overcame stewards to charge English fans. Public disorder was a major challenge for the Euro 2016 organisers, with French police having to deploy tear gas and water cannon to disperse crowds on a number of occasions. Moreover, after the violence between English and Russian fans inside the Stade Vélodrome in Marseille, French authorities admitted that there had been flaws in stadium security. The use of missiles and flares inside the stadium was an indication that the physical screening and bag search procedures had been weak.

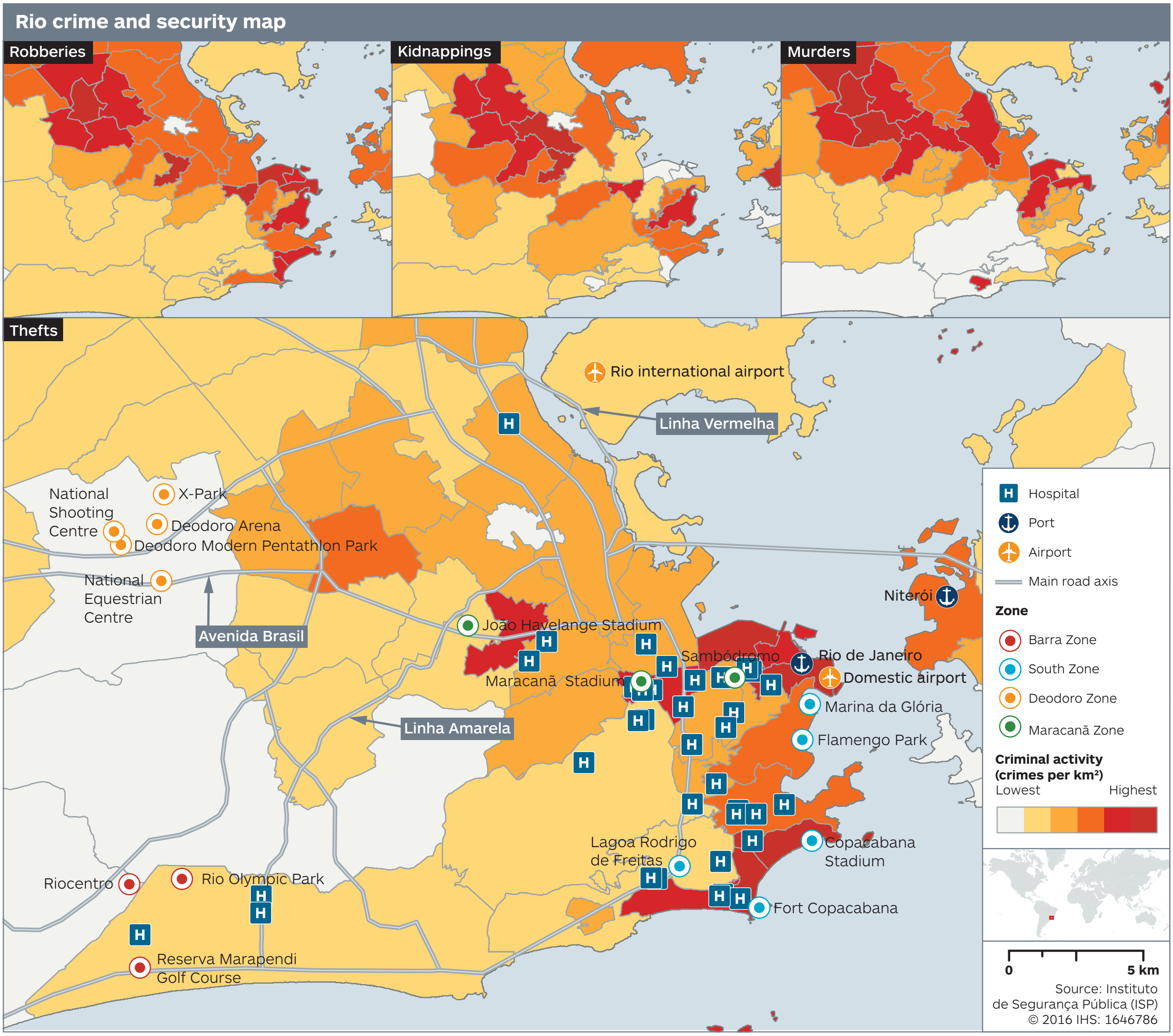
Security for major events with fans travelling from different countries requires international co-operation between police and intelligence services to identify and act upon potential threats. UK police provided intelligence to French authorities and issued up to 2,000 banning orders to prevent identified hooligans from travelling to the championship. However, according to French prosecutor Brice Robin speaking at a press conference in Marseille on 13 June, most of the Russians who caused trouble were known hooligans whose passports had not been confiscated by the Russian authorities.

Unrest of this nature can divert resources away from where they are required, and robust command-and-control (C2) policies need to be in place to assign or redirect assets if there is a change in the tactical situation.

The security threats facing the Olympics are different from those affecting Euro 2016. Brazil is not militarily involved in the Middle East and does not have a domestic terrorist presence, so the risk of a large-scale terrorist attack is lower than that of Euro 2016. The main challenges faced by the security services at the Olympics are likely to be street robbery and violence rather than mass-casualty attacks.

In addition, the saturation of security forces

Rio crime and security map



Source: Instituto de Segurança Pública (ISP)
© 2016 IHS: 1646786

will help to reduce the threat of crime to foreign visitors during the course of the Games. Indeed, the epidemiological risk posed by the Zika virus is likely to be a greater threat to the success of the Games than terrorism.

According to official projections, in addition to the 300,000–500,000 foreign tourists expected in Rio, there will be up to 15,000 athletes and 45,000 volunteers present during the course of the Games. Security during the Olympics will be provided by police and military personnel, similar to the security operation that Brazil mounted during the 2014 FIFA World Cup.

Civil Police, Military Police, Civil Defence, and Federal Police will provide approximately 47,000 security personnel, supported by approximately 38,000 members of the armed forces. These personnel will be responsible for the security of the Olympic sites and surrounding areas, and an additional 9,700 members of the National Public Security Force will replace private security and work as stewards within the Olympic sites. Security around potential targets at the Olympics will be increased, with a particular emphasis on physical searches of visitors entering the venues.

Event security challenges

The challenges faced by the authorities in securing mass-attendance events are considerable. A layered approach with multiple overlapping fields that are designed to divert, absorb, delay, and dissuade attempts to penetrate security is required in order to provide in-depth defence.

US Department of Justice guidelines for law enforcement planning and managing security for major events emphasise the importance of a large "show of force" that acts as a deterrent to disruptive behaviour. However, the presence of substantial numbers of security personnel is not necessarily reassuring to the public. Use of plain-clothes operatives and a less visible security presence can contribute to a more relaxed atmosphere, making it easier for observers to identify visitors behaving suspiciously.

The attacks in Paris, and the lone-gunman attack on a gay nightclub in Orlando on 12 June that resulted in 50 fatalities, including the shooter, may indicate a possible new priority in the Islamic State's target selection, although the motivation for the Orlando attack remains uncertain and the exact role of the Islamic State equally ambiguous, if it were indeed involved. Attacks on crowded venues with limited entry and exit points carry the potential for greater numbers of casualties than open areas from which people can disperse with greater ease.

Of the six distinct attacks launched in Paris that killed 130 people, the majority of deaths (89) occurred in the Bataclan theatre when shooters opened fire on the crowd. To guard against attacks of this nature, the key requirement is to prevent weapons from being smuggled into the venue.

The UK's National Counter Terrorism Security Office (NaCTSO), working with the Association of Chief Police Officers (ACPO), published guidelines in 2014 for major events that include risk management, security planning, and physical security guidelines. The emphasis in these guidelines is on identifying potential threats, minimising risks, and controlling access to the event.

As large bodies of people queueing for security checks are a potential target, NaCTSO advises staging the process to ensure that security staff are given the opportunity to scrutinise every visitor on entry. This is similar to the approach used at Israel's Ben Gurion Airport, where a "passenger-oriented" security system is in place. Similar tactics have been used by UK police, with Behavioural Detection Officers deployed at ports and large events.

A former senior British Army officer with experience in security and penetration testing cautioned against the reliance on hi-tech solutions, telling *IHS Jane's* on 20 June that security services were "sometimes blinded by the illusion of technology, when in fact physical searches are an essential adjunct".

Most static security personnel are trained to carry out screening security roles and to report anything suspicious. Training and basic investigation – such as asking questions and ensuring that concerns are reported promptly to police – assist follow-up and can reduce false alarms.

Finally, the pre-deployment of specialist teams with their equipment at or near venues also enables rapid response to – and early assessment of – potential threats, with procedures enabling their covert deployment. Such teams need to communicate effectively with venue security commanders and counter-terrorism (CT) advisors assisting decision-makers.

Lessons from London

The 2012 London Olympics involved the UK's largest mobilisation of military and security forces since the Second World War and was the largest ever peacetime police operation in the country. The Ministry of Defence announced that up to 13,500 military personnel would assist with security at 150 training and event locations. The private security firm G4S was originally contracted in March 2011 to supply a 10,000-strong security workforce, including private security guards and volunteers. It subsequently admitted that the promised number could not be delivered, and an additional 3,500 extra troops were drafted in for security duties.

The team responsible for security during the London 2012 Olympics stressed the importance of gathering good intelligence for rapid analysis and action. The use of a combination of tangible security assets such as closed-circuit television (CCTV), automatic number plate recognition (ANPR), metal detectors, and physical searches enabled mobile investigative teams of experienced CT officers to act on intelligence and to reach any location on the Olympic sites within minutes.

The main operational C2 centre was based in London and staffed by representatives from police and security agencies. A strategic control centre at New Scotland Yard managed co-ordination between relevant agencies and the sub-control stations established at each Olympic site. In the run-up to the Games, the venues were subjected to thorough searches and locked down, with access strictly controlled through the use of airport-style metal detectors and visitor screening.

The main legacy of the London security operation was the establishment of command, control, and co-ordination mechanisms across multiple civilian and military agencies. This enabled information to be passed along the chain of command and rapidly actioned. Contingency planning by the Counter Terrorism Command, which sought to cover every conceivable scenario, required a detailed response for each eventuality.

The latest available technology was built into the construction, development, and management of the games, but technology has evolved rapidly since 2012 and transferable lessons from London are therefore more about the use of additional information and the challenges it may produce.

Enhanced technology also resulted in an increase in the number of sources of information available to decision-makers. The range of sources and routes of reporting meant that circular reporting, multiple repetition, and pure speculation were commonplace, with the significant majority of alerts being false alarms. These volumes could have been the product of the paucity of any real threat intelligence or information, or of the deployment of a large number of security personnel and increased public awareness.

Information management was critical. Senior decision-makers with CT advisors who could rapidly verify facts and dispel myths became a key factor. Technological sources were able to detect the presence of persons of interest (POIs) but not their intent, which – given the high-impact nature of the threat – often caused decision-makers to assume the worst possible scenario, even when the POIs were simply passing venues on the way to and from work or trying to watch the Games. A combination of initial investigation, prompt reporting, rapid response, and expert advice provided the best support for decision-makers.

In preparation for the Olympics, a programme of 'Testing and Exercising' that focused on high-impact threats was undertaken. Sophisticated cyber-security processes were also put in place to protect the Olympic networks, and proved capable of dealing with the very small number of significant cyber-attacks that occurred. However, the failure of G4S information technology (IT) systems, which contributed to its inability to train, recruit, and deploy sufficient staff, alongside website problems experienced by the official ticket vendor Ticketmaster, demonstrated

> **'Attacks on venues with limited entry and exit points carry the potential for greater numbers of casualties than open areas'**

Facial recognition

Technological advances in social media can potentially be a major asset to security services when trying to identify persons of interest. One such example is FindFace from N-Tech.Lab, a service that can search the Russian social media network VK (originally VKontakte) for people based on a single supplied image.

According to a 17 May 2016 article in the UK newspaper *The Guardian*, the founders Artem Kukharenko and Alexander Kabakov believed that the future for their service would be in law enforcement and retail. The service works by comparing an uploaded photo to the database of publicly available profile pictures on vk.com and providing likely matches, but advances in computer processing power mean that the logical next step for such services would be "live tagging" from camera phones or internet-connected CCTV.

The potential benefits of this kind of technology to the security services are obvious, but there are also issues of legality across a range of jurisdictions, data protection, and privacy.

When Facebook rolled out facial recognition software to more than 500 million users worldwide in June 2011, it provoked concern about the type of information that would be available, and the company was threatened with legal action in Germany for potential violations of data protection and privacy laws.

that large events can be disrupted by problems with commercial partners' technology. Given the significant increase in the complexity and volume of criminal attacks on commercial systems, this is an important area of vulnerability for protection.

Another area of technological innovation during the London Olympics was the use of social media. This played a significant role in the mobilisation of rioters and the police response during widespread rioting in various UK cities in August 2011, and as a result the police established an All Source Hub (ASH) to gather social media intelligence (SOCMINT) in support of the 2012 Olympics security operation. This provided a significant volume of information on the mobilisation of public protesters, their sentiment, and their intent. It also potentially enabled investigators to rapidly identify and communicate with witnesses in the event of an incident.

Richard Walton, commander of the Counter Terrorism Command during the London Olympics, told *IHS Jane's* in June 2016, "Sentiment analysis enabled us to respond to and prevent planned public disorder by radical and extremist groups and proved to be of immense value in the run-up to and for the duration of the Olympics, particularly during the two months of the Olympic torch relay".

However, social media is vulnerable to manipulation and exploitation, with false and fabricated information rapidly going 'viral' with significant effects. The London Olympic security team understood that SOCMINT therefore required careful handling and senior decision-makers needed to be aware of its vulnerabilities, with effective social media strategies developed to rapidly counter any false reporting.

Outlook

Live facial matching of known suspects is likely to be a major driving force in future security for large events, as security provision is primarily concerned with the prevention of incidents rather than reaction. It would be unrealistic to expect that all potential suspects could be identified and contained before gaining admission to an event, but this technology can restrict terrorist suspects' free movement.

In addition, software-based 'sentiment analysis' systems – used, among other applications, to identify planning for the disruption of public order on social media – are likely to become more responsive in the future, with an emphasis on monitoring potential radicals and incident prevention.

Walton summarised Counter Terrorism Command's learning from the Olympics to *IHS Jane's*. He said, "Major event security is best achieved by gathering good intelligence, then analysing and acting upon it quickly, supplemented by both a visible and invisible police presence on the ground. Decision-makers need to be supported by effective intelligence analysis utilising a multitude of modern surveillance tools linked to one command-and-control system.

"These technologies could include advanced CCTV, ANPR systems, movement analysis of known suspects, and bulk data searching of flight and other manifests, alongside additional covert surveillance methodologies."

The inclusion of a range of false alarms and rumours within the information feed of exercises could better inform senior decision-makers about the challenges that they may face, and the volumes and quality of information and intelligence that they may need to manage, while management of senior officers' appetite for information that may or may not exist emerged as a necessity at the London Olympics. Closer support from the private sector, particularly involving the larger US technology companies that dominate the internet, is likely to become of greater importance to intelligence agencies, as commercially available hardware and software become more difficult for law enforcement agencies to access. Technology providers such as Apple have positioned themselves as neutral carriers of data, but this aspiration to be apolitical places them between their customers and the intelligence agencies.

Moreover, with the increased threat of lone-actor attacks by terrorist sympathisers, signals intelligence (SIGINT) will increase in importance in the quest to detect potentially threatening online activity before attacks can be carried out. This nevertheless carries a risk of false positives, with intent being difficult to successfully prosecute.

This kind of attack by self-radicalised individuals will remain among the most challenging for the authorities to defend against, as the lack of communication between cell members means there is minimal scope for discovery through the traditional intelligence-gathering disciplines of SIGINT or human intelligence. ■

This article was first published online at ***ihs.com/janes*** *on 21 July 2016.*

On the web

- Paris attacks focus EU on intelligence failures
- Euro 2016 tournament faces terrorism threat
- Olympian effort - Providing security for major sporting events

Author
Anthony Brooks is a former British Army officer with expertise in crisis response, personal security, and threat analysis. Shaun Romeril is a former Metropolitan Police officer and was a senior CT advisor to the National Olympic Security Coordinator during the London 2012 Olympics.

ihs.com/janes