RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 069 – 29 May 2024

Securing the Spectacle: The Multifaceted Security Challenges of the Paris 2024 Olympics

By Kristian P. Alexander

SYNOPSIS

Several security challenges such as the risk of terrorist attacks, cyber-attacks, and domestic unrest make the 2024 Paris Olympics vulnerable. Organisers must strike a balance between implementing stringent security measures and maintaining the open, welcoming atmosphere that embodies the spirit of the Games.

COMMENTARY

The Olympic Games are not only a celebration of global sportsmanship but also a massive logistical endeavour that brings together nations in a grand display of competition and cultural exchange. As Paris gears up to host the Olympics from 26 July to 11 August this year, the city faces the formidable task of ensuring the safety of thousands of athletes, fans, and dignitaries amidst a complex security landscape.

Paris: A prime target

Paris's history with terrorism marks it as a high-risk target during the Olympics. The city has been the scene of several horrific attacks, including the January 2015 attack on the offices of Charlie Hebdo and the November 2015 attacks on a football stadium that collectively left 142 people dead. These incidents underscore the ability of terrorists to strike at the heart of French society and expose vulnerabilities within the nation's security infrastructure. The global visibility of the Olympic Games further elevates the risk, attracting the attention of terrorist groups that view France as a symbol of Western policies they oppose. ISIS and Al-Qaeda, in particular, have reasons to target France due to its involvement in military operations against these groups in the Middle East and Africa.

The evolving nature of terrorist networks, with a shift towards online radicalisation, makes lone wolf attacks—a scenario where individuals act based on extremist ideologies—a distinct possibility. Such attackers often require minimal planning and coordination, making them difficult to predict and prevent.

Political unrest increases risks

The current global political climate, marked by conflicts in Ukraine and Gaza and significant upcoming elections, could further exacerbate the security situation. France has experienced its share of domestic unrest, notably with the riots in Nanterre in June 2023 following a police shooting. This unrest highlights the broader social issues of unemployment, poverty, and exclusion, particularly in suburban areas known as *banlieues*, where young people, may feel marginalised from mainstream society. These conditions not only foster domestic unrest but also serve as breeding grounds for radicalisation.

The sense of alienation felt by these young individuals in the banlieues can make them susceptible to online propaganda. Extremist groups often target such vulnerable populations through social media and other online platforms, offering them a sense of belonging and purpose in exchange for allegiance to their radical causes. This digital indoctrination can be particularly potent during global events like the Olympics, where the convergence of international attention and local tensions can escalate feelings of disenfranchisement.

Moreover, the Olympics' demand for a large workforce could inadvertently provide these radicalised individuals with easier access to the event's venues and infrastructure. Many young people from these marginalised communities might find employment opportunities as volunteers or employees within private catering and event management companies contracted to service the Games. This employment, while beneficial in providing work, could also pose a security risk if individuals with radical sympathies are placed in sensitive or critical roles without adequate vetting.

Cyber-attacks: An ever-present risk

The digital transformation of the Games, expected to draw an audience of four billion people, introduces significant cybersecurity risks. The Paris Olympics, with its extensive digital footprint from access badges to surveillance systems, presents a lucrative target for cybercriminals. Past events have shown the extent of potential cyber threats: the 2008 Beijing Olympics were targeted by Operation Shady RAT, a sophisticated hacking operation, and the 2016 Rio Olympics were compromised by Russian hackers who leaked athletes' private health data. Malicious hackers have the potential to target critical infrastructure, including power grids, transportation systems, and communication networks.

A successful attack on any of these could lead to widespread disruptions, paralysing the logistics that are crucial for the Games. In addition, there is a high risk of data breaches involving personal information from athletes, officials, and spectators. Such breaches not only compromise privacy but also open the door to identity theft and various forms of financial fraud. Another pressing cyber threat comes from ransomware attacks, which could infiltrate and lock down essential systems, demanding large ransoms to restore access. These attacks could delay, or interrupt scheduled events, creating chaos, and undermining the integrity of the Games.

Security Strategy and International Cooperation

To address these multifaceted security challenges, French authorities are implementing a comprehensive, multi-layered security strategy. This strategy involves deploying approximately 45,000 police officers and up to 20,000 military troops, supplemented by around 20,000 private security personnel. The sheer scale of this mobilisation underscores the complexity of securing the Olympics. Security measures will extend beyond the venues to include transportation systems and hotels, ensuring a security perimeter that covers all areas where participants and spectators will congregate.

Effective crowd management and rapid response to emergencies are critical components of the security strategy. Advanced surveillance technologies, including CCTV, facial recognition systems, and drones, will play a vital role in monitoring for suspicious activity.

Physical security measures, including perimeter fencing, vehicle barriers, and security checkpoints, are crucial in controlling access to Olympic venues and reducing the risk of unauthorised access. Additionally, specialised security forces such as counterterrorism units and bomb disposal squads will be strategically deployed onsite. These teams are trained to quickly address and neutralise any security threats, ensuring a rapid response to incidents ranging from potential terrorist activities to safety breaches.

French President Emmanuel Macron has even indicated that contingency plans are in place to relocate the ceremony to a more secure location, such as the Stade de France, if a security threat arises.

Striking a balance between security and the spirit of the Games

Organisers must strike a balance between implementing stringent security measures and maintaining the open, welcoming atmosphere that embodies the spirit of the Games. This balancing act also raises critical issues regarding privacy and civil liberties, especially with the integration of advanced security technologies that may involve mass surveillance and movement restrictions.

To safeguard the vast influx of athletes, officials, and spectators, organisers are likely to deploy sophisticated surveillance systems. These can include facial recognition cameras, drone surveillance, and extensive data collection tools that monitor movements and potentially gather personal information on a mass scale.

Such measures, while effective for security purposes, raise significant concerns about privacy. The use of surveillance technologies can lead to the collection of large amounts of personal data without explicit consent, potentially violating individual privacy rights. Moreover, these systems can retain data longer than necessary or use it for purposes other than security, leading to further encroachments on privacy.

Additionally, the implementation of movement restrictions, possibly through geofencing or other location-tracking technologies, can impinge on civil liberties. These restrictions might limit freedom of movement or lead to discriminatory practices if certain groups are targeted more than others.

Conclusion

The task of securing the Paris Olympics involves a dynamic interplay of addressing both traditional security threats and modern challenges such as cybersecurity and political unrest. The extensive security measures planned reflect a proactive approach to safeguarding the Games, ensuring that the event not only proceeds smoothly but also retains the core values of unity and global harmony that the Olympics strive to promote.

Dr Kristian P. Alexander is a Senior Fellow at the Rabdan Security & Defense Institute (RSDI), Abu Dhabi, UAE.