On the Convergence of Physical and Digital Security for Public Safety at Olympic Events

Chris. W. Johnson, DPhil;
Department of Computing Science, University of Glasgow, Scotland, UK.

Keywords: Olympics; Safety; Security; Lessons Learned.

Abstract

It is increasingly difficult to distinguish between the digital and physical systems that protect public safety at Olympic events. In the past, computer networks were used primarily to store results and to coordinate logistics for major sporting competitions. They carried relatively limited information about the direct physical security of spectators and participants. However, the Athens games began to use digital infrastructures to carry images from surveillance cameras using the MPEG4 format across Asynchronous Transfer Mode (ATM) switches. The Beijing Olympics will introduce sophisticated monitoring algorithms including facial recognition and pattern detection in public places. There are also plans to use Radio Frequency Identification (RFID) tags and the Global Positioning System (GPS) to monitor diverse aspects of the Games, including the physical movements of spectators and athletes. The intention behind these initiatives is to direct physical security teams against international and domestic threats that range from Islamic terrorists though to environmental protestors. The following pages identify a number of concerns about the integrity of these systems. Previous physical attacks at Munich and Atlanta have shown the importance of preparing for contingencies including direct attacks on the security infrastructure. Reported threats from employees or sub-contractors against the Turin networks illustrate further concerns over digital security. All of this must be placed in the context of increasing complexity both in terms of the Games themselves and in terms of the diverse computational systems that must be integrated to protect public safety. It remains to be seen whether the planning teams for Vancouver (2010) and London (2012) have learned the lessons that previous failures in physical security provide for the development of digital security at Olympic events.

Introduction

In the past, digital systems were isolated from the physical security of Olympic events and, therefore, did not have much impact on public safety. They provide necessary logistic support and provided means of communicating the results from sporting events distributed across large geographical areas. Increasingly, however, computer networks are being integrated with sensing technology to inform and direct the physical security of the Games. The following pages use lessons learned from previous failures in physical security to encourage organising committees to consider what might happen to public safety if these systems are compromised either by external attack, disaffected insiders or by technical failure (Johnson, 2006).

Munich 1972: Public Access, Safety and Physical Security

A number of previous incidents illustrate the tension that exists between physical security, public safety and access to Olympic events. Each of these adverse events has forced organizing committees to rethink the mechanisms and policies that can be used to regulate access to key venues. Organizing committees must continually trade off increased security measures against the need to protect the 'spirit of the games'. The potential conflict between these two objectives can be illustrated by the kidnap of eleven Israeli athletes and coaches from the Munich Olympic Village on the 5th September 1972. The attack was coordinated by the 'Black September' faction of the Palestine Liberation Organization. At 04:40, 5 terrorists climbed a 2 meter fence wearing tracksuits and carrying weapons concealed in athletics bags. They joined 2 other sympathizers who had security credentials and were already inside the Olympic village. The group gained access to the Israeli team's apartments using two keys. Three team members escaped, four other athletes, two team doctors and the delegation-head managed to hide. A coach and an athlete were killed as they tried to delay the attackers. A further nine Israeli team members were taken hostage. The terrorists demanded the release of 234 prisoners in Israeli jails. They also asked for Andreas Baader and Ulrike Meinhof, from the Red Army Faction to be freed from a Frankfurt prison. By 15:50, the games had been suspended. A political decision was made not to accept an immediate offer of assistance from Israeli Special Forces. It was subsequently claimed that many of the security teams who were used by the Germans lacked specialist training in anti-terrorist operations.

These initial events reinforced the importance of physical separation as a key component of Olympic security. The ease with which the terrorists were able to gain access to the Olympic village provided important lessons to all subsequent organizing committees. Since then, perimeter security has been reinforced with the use of constant patrols, of night vision technology, audio sensing devices and the use of CCTV cameras with software enhanced surveillance including automated detection algorithms. These mechanisms have helped to implement layered or zoned policies where only those individuals with the highest levels of security can gain access through successively more stringent checkpoints. The London and Sydney committees followed this policy by incorporating the athlete's village inside the perimeter of their Olympic parks. However, as we shall see, several of the lessons provided by the Munich attack have not been learned by some organizing committees. In particular, the 'insider threat' continues to pose significant problems, especially when those individuals have access to key components of the infrastructure such as the underlying computational systems which did not exist at the time of the Black September attack.

By 17:00 German police had been deployed around the building dressed in tracksuits. Members of the terrorist group leaned out of the apartment building to observe teams whose location had been shown in television coverage. With little prospect of successfully storming the building, the German authorities reached an agreement with the terrorists to allow them to board a plane for Cairo. A plan was developed to disguise six police officers as attendants on a decoy plane. They were to overwhelm any terrorists who inspected the aircraft while snipers fired on those who remained with the hostages. However, the team on the plane had little or no training in special operations and voted to abort the mission without reference to the control group. The two terrorists who went to inspect the decoy plane discovered that it was empty and ran back towards the hostages. The snipers had been selected for their marksmanship and had no experience of hostage situations. They lacked radio equipment, protective equipment and telescopic sights. At least one sniper was wounded by a fellow police officer and the authorities rapidly lost control of the situation. Several terrorists were shot. However, the hostages remained tied up on the tarmac as the remaining kidnappers began to shoot out the airport lights, killing a policeman in the control tower.

It is important not to criticize the German authorities with the benefit of hindsight. At the time, many counter terrorism techniques were still being developed. Subsequent events have used the insights from1972 to reorganize the physical security of the Games, for example by ensuring support from specialist counter terrorism agencies. However, if we look beyond physical security to consider the digital infrastructure of the games it is less clear that we have learned from the Munich attacks. The plans for a rapid response to IT infrastructure contingencies are less developed than those for physical security. For example, previous committees have not conducted the sustained drills that are needed to verify their potential response following a successful attack on the public information systems or results monitoring applications. Similarly, it is unclear what would happen to physical security if digital security infrastructures were compromised. Organizers would have to deploy significant physical security resources to make up for the loss of sensor networks, CCTV and audio monitors, as well as public security functions, including the loud speaker systems that have been multiplexed onto security camera networks in previous games. The difficulty of identifying the extent of any attack, where breeches of digital security may leave little evidence of any intrusion, makes it critical that organizers consider the technical and organizational mechanisms that are required in order to determine the level of risk posed by any attack. Otherwise there is a danger that we will be struggling to respond in the aftermath of a breech in digital security just as the German authorities were forced to improvise their response to the Munich attacks.

Atlanta 1996: Public Access, Safety and the IT Infrastructure

The attack on Centennial Park during the 1996 Summer Games in Atlanta provides a direct illustration of the importance of a 'systems approach' to public safety. As we shall see, the response to the attack was significantly delayed not by problems in the computational systems created by the organizing committee but by flaws in a police dispatch system that had not previously been recognized as a core component of the Games infrastructure. The Atlanta Centennial Olympic Park was used for concerts, exhibitions and a range of corporate events. At approximately 00:58 on the 27th July a security guard noticed a green rucksack underneath a bench. He alerted a bomb disposal team and with a Georgia Bureau of Investigation agent began to clear people away from the immediate area. At 01:07, a male voice told called 911 and stated: "There is a bomb in Centennial Park, You have 30 minutes." The operator then followed standard operating procedure by trying to dispatch police teams to the venue. In order to do this they had to enter the location of the Park into the 911 dispatch software. The operator was unsure of the address for the venue and could not enter the name directly into the system. She tried to call the

Police Department's Agency Command Center but their lines were busy. It was subsequently argued that organizers had underestimated the number of staff and other resources necessary to deal with relatively minor public order incidents created by the Games in the early hours of the morning. The 911 operator then called the police precinct where Centennial Park was located:

911 operator:	"You know the address to Centennial Park?"
Police dispatcher:	"Girl, don't ask me to lie to you."
911 operator:	"I tried to call ACC but ain't nobody answering the phone. ... but I just got this man called talking about there's a bomb set to go off in 30 minutes in Centennial Park."
Police dispatcher:	"Oh, Lord, child. One minute, one minute... uh, OK, wait a minute, Centennial Park, you put it in and it won't go in?"
911 operator:	"No, unless I'm spelling Centennial wrong. How are we spelling 'centennial'?"

The operator again tried to contact the Police Agency Command Center and was given a further phone number to call. These delays further hindered the response to the bomb threat and prevented additional resources being deployed to help evacuate members of the public from the venue:

911 operator:	"I need to get this bomb threat over there to y'all."
Police Agency Command Center:	"Well."
911 operator:	"But I need the address of Centennial Park. ... that's where he said the bomb was."
Police Agency Command Center:	"No particular street or what?"
911 operator:	"He just said there's a bomb set to go off in 30 minutes in Centennial Park."
Police Agency Command Center:	"Ooh, it's going to be gone off by the time we find the address."
911 operator:	"Are you kiddin'? Give me that, give me that."

Atlanta provides an important lesson for future Games where emergency services rely on legacy computer systems that cannot easily be updated with the names and locations of venues which are often built specifically for an Olympic competition. In other words, this attack provides an important illustration of the key argument in this paper. It is increasingly difficult to separate physical and virtual security concerns in the preparation for Olympic events. In this instance, changes to the physical venues used by Olympic events were not reflected by changes in the information infrastructure used by the emergency services. The dispatch software did not recognize the new names that had been given to Olympic venues. Public safety depends upon a more integrated approach than has been seen in previous Games. Planners also arguably failed to consider a wide enough range of physical targets associated with entertainment and sponsor's events rather than sporting venues. It can also be argued that security teams could have analyzed a broader range of digital infrastructures during the planning for the Games. The FBI concluded that risk assessments did not recognize the police dispatch system as a key component in the response to terrorist attacks. The pipe bomb exploded at 01:20 killing two people before the Park could be cleared. Atlanta hospitals implemented their emergency response plan and began to deal with the 110 injuries. At the same time, police units acted to seal off downtown Atlanta trying to catch the perpetrator.

The attempts to catch the attacker were unsuccessful and suspicion began to focus on the security guard who initially discovered the device. It took many months before those suspicions were shown to be groundless. In the meantime, there remained the possibility of further attacks. This has strong parallels in the area of digital security where it is increasingly difficult to identify potential perpetrators. It is far simpler to identify that a physical intrusion has taken place than it is to step back through successive layers of indirection and proxies to identify the source of a digital attack. This is a particular concern given the political significance of the Games and that the source of an attack may, therefore, be supported not simply by the usual terrorist or individual motives but also by the financial and technical resources of foreign governments. There are further parallels between physical and digital security. The local organizers decided to delay the evacuation of the Park in order to avoid panic. Organizing committees have also been reluctant to publicize attacks on digital infrastructures in order to avoid undermining public confidence.

The decision not to release information about potential threats on both physical and digital security is further justified by the potential threat from copy-cat attacks and from hoax calls. Scarce resources can also be wasted following up reports of security concerns that often prove to be ungrounded. More than 100 reports of suspicious packages were made in the 24 hours following the explosion in Centennial Park. All proved to be harmless. These incidents placed immense stress on the police and other security agencies. For example, a suspect package led to the evacuation of thousands of people from the 'Underground Atlanta' shopping mall. This was next to the Five Points interconnection for the city's rapid transit system. Thousands more people were affected when this main north-south and east-west transfer point was closed. The paradoxical effect of increasing public awareness was that the sheer number of false alarms may have created opportunities for subsequent malicious acts. Recent bombings, for example on Baghdad University, have relied upon synchronized techniques; a small initial device is detonated or a hoax call is used to trigger an initial evacuation. Suicide bombers are then used to attack the crowds that gather in the assembly points outside the initial building.

The consequences of any attack, whether it is on the physical or digital infrastructure of the Games, can undermine the confidence of everyone involved in the event. Following the bombing at Centennial Park, security teams had to prepare for the following day's events with relatively little information about who might have planted the device or whether there would be another attack. Standard Operating Procedures were reviewed in hours following the explosion. Searches were increased; cordons extended, luggage was banned from key venues. Steps were also taken to increase public confidence; the media covered the deployment of 9,000 national guards. The park was closed for three days while officials investigated the bombing and was reopened after a brief commemorative service. Although we have yet to experience a major breach of Olympic digital security, the consequences are likely to be just as severe. It is notoriously difficult to ensure that the source of any violation has been eradicated once an intrusion has been detected. It may then be difficult for event organizers to trust the results presented on the internal data systems. Similarly, it would be hard to restore the confidence of security personnel in the future resilience of information systems if an attack were ever to be successful on the digital networks that increasingly carry critical monitoring data and command information between staff distributed across multiple venues.

Sydney 2000 and Salt Lake City 2002: Public Safety, Paranoia and the Boundaries of Defense

The Sydney 2000 Summer games benefited from many of the lessons that were learned in Munich and Atlanta. Public venues were brought within the perimeter of an Olympic park, although the Black September attack showed that this may not always offer protection to the public and participants. Bag checks and metal detector cordons were introduced to support the zoned security policy. 20,000 soldiers, reservists, police officers and volunteer security officials were also recruited. Concerns were focused on two main threats. The first centred on public protests from following sustained clashes between Australian police and anti-capitalist demonstrators in Melbourne shortly before the games. The second area of concern focused on international instability motivated by the conflict with the Taliban in Afghanistan. A group of Afghanistan students were arrested by the New Zealand police shortly before the Olympics. Although they were initially suspected of involvement in a people smuggling operation, this group was found to possess plans for the Lucas Heights reactor near Sydney. It is difficult to assess the plausibility of any security threat that is not realized. However, the possible consequences of the Lucas Height incident continue to influence subsequent hazard assessments for Olympic events.

Risk assessment continues to be advocated as the primary means of controlling security costs by focusing resources on those threats that are assumed to carry the highest potential consequences and highest likelihood of attack. However, these assessments cannot easily be sustained against the unpredictable nature of directed terrorist actions and the ever changing nature both of the Games themselves and the technological infrastructures that they depend upon. Olympic security committees are faced with an increasing range of scenarios. Initially most attention focused on the actions of organised and well known political groups following the events at the Munich games. Resources were then targeted towards the actions of 'loners' and dissident groups following the FBI enquiry into the Atlanta bombing. Lucas Heights renewed concern over potential Chemical, Biological, Radiological, and Nuclear (CBRN) attacks on Olympic venues and neighbouring areas. It is impossible to protect every possible target against all potential threats as security costs continue to escalate. Similarly, there are particular events, including the Marathon, which pose almost insurmountable challenges. In the digital domain, it is equally difficult for organising committees to identify the extent of any hazard. In the past, there was little need to create multiple computer networks because the Games management systems were primarily dedicated to event organisation rather than security related data. However, digital infrastructures now support every aspect of Olympic organisation from

catering through to the rostering of security teams. New threats are also emerging, for example, as coaches and competitors try to connect their personal laptops to the secured networks. This has happened at every Games since Sydney even though all participants have been warned of the potential problems they can create. 802.11 wireless networks continue to be detected near major venues with spectators and athletes searching for ad hoc Internet connections.

The 2001 attacks on the Pentagon, World Trade Center and Flight 93, convinced the organizers of the 2002 Salt Lake City Winter Games to increase their security budget from $300 million to $334.5 million. This helped to fund more than 7,000 federal, state, military and private security personnel. Rucksacks and large bags were banned from all Olympic sites. Vehicles were prohibited within 300 feet of the venues and other designated buildings. This further extended the physical scope of Olympic security concerns identified in the previous paragraphs. A similar trend can also be seen in growing use of digital networks to protect public safety. The Salt Lake City security teams used portable X-ray devices to scan suspicious mail packages. Package tracking applications were monitored to identify the routing for particular items. Biometric scanners were also introduced to identify athletes and officials. These systems received updates over secured networks. However, the 2002 Games also revealed the limitations of using digital systems to support physical security. Accredited team members were refused entry to key venues when the software failed to identify the biometric information provided at checkpoints. This created significant delays and required tact on the part of the security teams that had to interact with participants under considerable stress prior to competition.

During the Salt Lake City Games, the Utah Olympic Public Safety Command ran security operations through an Olympic Coordination Center. This provided a focal point for the mass of information that was gathered by a range of safety and security organizations. The FBI was responsible for crisis management, investigating and preventing terrorist threats and apprehending those responsible. They also operated a mobile field laboratory to detect any potential radioactive, chemical or biological weapons. The Federal Emergency Management Agency was to coordinate the federal response to any incident. They also provided a National Emergency Response Team and several Urban Search and Rescue Task Forces. The US Customs Service was responsible for securing the airspace. The Department of Defense provided approximately 5,000 military personnel to support logistics, communication, air transport and explosives identification. The US Immigration and Naturalization Service provided 200 Border Patrol Agents to secure the Olympic venues. The U.S. Marshals Service, the Bureau of Alcohol, Tobacco and Firearms, the Department of Energy, the Environmental Protection Agency, the Department of Health and Human Services, the Center for Disease Control, the Food and Drug Administration, the Forest Service and National Park Service, the Department of Transportation all provided personnel and data that contributed to the Salt Lake City security systems. The complexity of integrating these different organizations can only be imagined and, in part, explains the decision to establish a Joint Information Center in the State Capitol Building to provide a 'one stop shop' for public safety information. The underlying digital networks that supported the exchange of safety and security data mirrored the organizational complexity.

A command post exercise was organised by the FBI during November 2000 to determine whether the new communications infrastructure could cope under a simulated emergency. The analysis of digital systems was mirrored by evaluations of physical security using a Field Training Exercise in April 2001. This involved more than 1,600 security staff across several venues. It used simulated terrorist assaults, hazardous materials incidents and crisis management drills. However, the difficulties of a 'systems' approach to public safety at Olympic venues cannot be underestimated. Recent games have experienced considerable problems in ensuring that venue construction is completed with sufficient time for security agencies to conduct large scale drills using a range of different attack scenarios. In consequence, virtual exercises have often provided most of the testing for critical infrastructures with more limited opportunities to test communications and coordination mechanisms on site in the final days leading up to the Games.

Athens 2004: Eroding Distinctions between Digital and Physical Security

The invasion of Afghanistan in October 2001, the attacks in Bali and the Moscow theatre siege in October 2002, the second invasion of Iraq during March 2003, the al-Aqsa or second Intifada, the Madrid train bombings in March 2004 have all heightened concerns over public safety at Olympic events. These threats combined with more local worries for the Athens Summer Games in 2004. For instance, the 'Revolutionary Struggle' terrorist group used explosives to destroy an Athens police station during May 2004. The group justified their actions as a demonstration

of the vulnerability of the games and as a protest against business interests linked to the Games. These local and international threats raised security costs to €1 billion. This was more than 10% of the total direct costs and almost four times greater than the security expenditure for Sydney in 2000. These trends raise important questions for future Games. Beijing (2008) can call on a state infrastructure that is not available to Vancouver (2010) and London (2012). There were approximately twice as many security personnel available in 2004 compared to the summer games four years before. The Athens organizing committee could call on 21,000 police officers, 3,300 coast guards, 1,400 fire personnel, 7,000 Special Forces, 2,800 private security staff and 5,600 security volunteers. Organizing committees will have to determine whether it is possible to sustain such large security teams, given the communications overheads and coordination problems that were exposed by both the Munich and Atlanta attacks.

Overall responsibility for the security of the Athens Olympics belonged to the Hellenic Police under the Ministry of Public Order. They created a dedicated police unit known as the Olympic Games Security Division, which set up an Olympic Intelligence Centre (OIC) similar to the Joint Information Center from Salt Lake City. The OIC was responsible for the collection, analysis, and assessment of intelligence relating to the Games. It coordinated threat assessments and was intended to help share information with more than 150 countries and international organizations. These ranged from the data provided by NATO Airborne Warning And Control System aircraft through to the risk assessments provided by an international Olympic Security Advisory Group. At the same time as the organizational complexity of the Games steadily increased, Athens saw the development of one of the most complex technical infrastructures for any sporting event. The data networks helped to merge continuous streams of video, audio and data from 63 command centers with 1,250 operators, monitoring 47 venues over an area of 250 square kilometers. Technical solutions involved MPEG4 digital surveillance cameras using video over the Internet Protocol (IP) with Asynchronous Transfer Mode (ATM) switching. Operators were able to use speakers attached to surveillance cameras to make public safety announcements. This digital architecture supported access control software that monitored the privileges associated with different stakeholders. Multiple agencies including the Police, Coast Guard and Military could draw feeds from the system that only provided access to information within their particular area of concern. Local users were granted permission to access cameras at their venues while higher levels of management could survey several different locations. A distributed architecture also provided redundancy and resilience in the face of partial network failure. However, the technical innovation and scale of the command and control systems led to considerable delays. The Athens Olympic Games Security Division held seven major drills before the Games; these included a simulated chemical attack, a plane hijacking and an epidemic outbreak. However, the Greek organizing committee had planned an ambitious construction programme around the various venues. Delays in construction prevented some of the exercises from being staged. Development problems also delayed tests that were designed to validate information systems at several key locations. A Greek delegation was sent to Washington to calm fears over these issues and to ensure continued US participation.

The previous paragraphs have described how digital security systems are increasingly being used to inform and direct physical countermeasures at Olympic venues. However, the Athens games again illustrates the vulnerability of major sporting events. A marathon runner was held to the ground for several seconds by a former Irish priest while he was leading the marathon. He eventually completed the remaining 3 miles and finished in third place. The president of the Brazilian Olympic Committee criticized the security measures stating that the lead runner should always be flanked by at least two motorcycles. This attack illustrates how even the most sophisticated digital infrastructures cannot ensure the complete safety of competitors and the public during Olympic events. It is a useful reminder not to become so dazzled by technological sophistication that we ignore the more direct threats posed to the Games.

Turin 2006: Militant Islam, Globalization, the Environment and the Winter Games

The organizers of the Turin Winter Olympics in 2006 faced a local and international picture of potential threats that was every bit as complex and those that faced their predecessors in Sydney, Salt Lake City and Athens. Wire-tap evidence and a Tunisian informer led to the arrest of 3 North Africans for planning to bomb part of the Milan Metro in February 2004. The Italian courts had also sentenced three Tunisians, an Algerian and an Egyptian to between 4 and 8 years for arms possession and making false documents. There were strong similarities between these various groups and those involved in the London bombings of 7th July 2005. The organizers were also worried about local groups, including the Informal Anarchists Federation, opposed to Olympic sponsorship by major corporations. There were up to 60 sporadic attacks against government and infrastructure targets during 2005. Most involved improvised explosives and were intended to raise publicity without causing injury.

The Turin security committees also had to consider a range of environmental protests linked to the new TAV (Treno ad Alta Velocità) high-speed railway line. Initial demonstrations were peaceful; however, they quickly led to clashes. On the 6 December 2005, Italian riot police attempted to break up a protesters' camp at Venaus. Activists responded by blocking the A32 autostrada between Turin and Frejus. Flares were thrown at the official Olympic shop in the Piazza Castello in Turin. Protests against the TAV and the Olympics came together in more than 30 demonstrations along the route of the Olympic flame. In 2006, the torch acted as a focus for diverse protest groups ranging from Campaigners for a Free Tibet to Anti-Globalization demonstrators. The diversity of these threats has justified the development of increasingly complex intelligence networks. The intention is to provide organizers with the information that is necessary to guide the allocation of scarce security resources. In consequence, the organizing committee of the Turin games increasingly referred to the computational or digital infrastructure as the 'guiding agency' for physical security countermeasures.

The 2006 winter Games were managed by a committee known as TOROC (Torino Organizing Committee 20th Winter Olympic Games). TOROC's Safety and Security Committee established a Gruppo di Pianificazione della Prefettura with local agencies to plan the deployment of surveillance cameras, metal detectors etc. It also helped to develop requirements for infrastructure provision and the security technology necessary to implement access control policies. During initial planning, TOROC's Security and Safety group employed about twenty security experts. By the start of 2006, this core group had grown to around 40 employees each working in four different teams. The first dealt with security technologies, training and coordination of volunteers, planning transport and the logistic of security. The second team focused on communicating safety information between TOROC and external agencies, including National Olympic Committees and Sponsors. The third group focused on security arrangements for competition venues. The fourth, and final, team demonstrated that the Turin organisers' had learned some of the lkessons from Atlanta by focusing on the security and safety of 'associated venues'. In addition to the centralized security organization associated with the sub-groups in TOROC, each site had a Security Manager who implemented Security and Safety group plans under the operational supervision of the Public Security Forces.

Digital security for the Turin Winter Olympics was coordinated by the IOC's preferred 'Worldwide Information Technology Partner'. They employed more than 2,000 people to maintain the IT infrastructure for the Games using 385 servers, 5,000 computers, 700 printers, and 22,000 miles of cable. Over 100,000 person hours of testing were used to assess the security and reliability of the networks. IT infrastructure was based around two separate systems: an Information Diffusion System (IDS) and a Games Management System (GMS). The IDS provided event information to spectators and media outlets worldwide. The GMS linked physical ID badges with access information for more than 100,000 athletes, coaches, officials, media representatives, staff, law enforcement and emergency personnel. However, the principle networks were isolated from the Internet and all devices attached to the network had to be submitted for inspection and approval. Intrusion detection systems issued an alert if an unauthorized device was connected and the device was automatically disconnected from the network. A response team was then dispatched to the physical location associated with the alert. During the 16 days of the Games, almost five million security alerts were logged. 425 were classified as serious and 20 were critical. These included accredited people attempting to disconnect devices from the Games intranet so that they could connect a personal laptop to the Internet. Such events were treated seriously following a risk assessment that had identified the threats posed by viruses as well as the falsification of event results and attempts to access information about the security provision at key venues. Digital attacks might also have compromised a range of sensitive data including personal information about the competitors, the itineraries for heads of state and other VIPs etc. Concerns over data integrity were heightened by claims that one of TOROC's technical consultants had compromised network security. TOROC issued a press statement to counter these claims; "This consultant, who is now a former consultant, said in a very strong way that he could do certain things to the network. Nothing has happened and all the passwords have been disabled". No charges appear to have been filed against the individual.

Beijing 2008:

At first glance many aspects of the digital and physical security plans for 2008 look very similar to those of other recent Olympic events. Beijing has planned to allocate some $300 million to Olympic security, about one fifth of the total investment. This will contribute towards the costs associated with 90,000 policemen. Beijing has also established an organizational framework for security that resembles those of Turin and Salt Lake City. In December 2004, the Olympic Security Control Centre was established with seven departments to plan for specific

venues, participants' accommodation, transportation etc. Other aspects of the planning are also familiar. The security organization has been directed by a risk assessment that was initially developed when the Chinese government backed their bid to host the Games in 2001. This analysis considered potential fire hazards, illegal 'invasion' of Olympic buildings, urban turmoil, common crimes, technological problems, traffic safety, natural disasters and terrorist activities for each proposed venue. The consequence analysis considered both the layout of the venue and potential ticket sales. These initial risk assessments were reinforced by an international security conference in November 2006 where anti-terrorism experts from reviewed security measures for 2008. The meeting recognized the radically different political and social context for the Beijing Games, compared to Sydney or Athens. However, the Chinese authorities continue to assume that they could be a target for Al-Qaeda as well as what they term the 'traditional' school of terrorism. This includes the East Turkestan Islamic Movement (ETIM) advocating an independent Xinjiang as well as Tibetan separatist organizations. Further concerns focus on the growing divides between rich and poor, rural and urban Chinese, which might conceivably trigger terrorist acts during the Olympics.

Further parallels between the Beijing games and previous Olympic events can be seen in the use of security zones that were also a feature of Turin and Sydney. However, these are being extended. Current plans provide for the initial supervision of participants and spectators up to10 kilometres from each venue. X-ray machines are being deployed to every entry point of all major stadia. Beijing is also holding drills and exercises that seem similar to those described in previous paragraphs. However, they are taking place significantly earlier than has been possible in previous competitions. For example, one recent anti-terror simulation was staged in Qingdao, the venue for sailing events, during December 2006. Few details have been released although speculation exists that it focused on a biochemical strike on the city.

The Beijing games takes place in a radically different social context than recent Games. This has an impact on security planning. For instance, 'grandpas and grandmas' wearing red armbands will scrutinize local communities to identify potential trouble makers before events take place. State control will also be more direct and this may simplify the task of the organising committee. However, the pressure to innovate and demonstrate new security systems can be seen in China just as it has been in Greece, Italy, Australia and the USA. The for technical innovation is driving the further integration of digital networks into the physical infrastructure that protects public safety. Security planning centres around five key systems: video monitoring; building sensors and alarms; the access control system; the electronic ticketing system and the security detection system. Between 2001 and 2008, the security investment in the 'Grand Beijing Safeguard Sphere' is estimated at $6.5 billion. Most of this will support the development of the Beijing video monitoring system with funds being provided by financial organizations, universities, large-scale shopping malls, hotels, internal enterprises and residential communities. The cameras being deployed into the Olympic venues feed into this system. The additional infrastructure enables the municipal public security bureau and all district sub-bureaux to access real time images. In the past, these organisations relied on radio communication. The camera infrastructure provides the backbone for IBM's Smart Surveillance System (S3). S3 can be used analyse and index digital video recordings. Software automatically warns security guards when someone has entered a secure area or when particular traffic patterns have been identified. The infrastructure is similar to that pioneered in Athens with the ability to patch both analogue and IP-based cameras into the system. The novelty lies in the use of algorithmic support to identify potential security concerns and then direct physical interventions. It remains to be seen whether the high false positive rates that have weakened previous applications will also affect this system.

The social context for the Beijing Games not only supports Olympic security, for example by providing state resources at a level that might otherwise be difficult for other venues. The social context also creates particular challenges for the Chinese government. In particular, the Olympics will attract an influx of overseas visitors that might otherwise threaten to overwhelm existing state infrastructures. There will be up to one million additional spectators and more than 200,000 overseas staff associated with the Games. The FBI has also developed a 'shopping list' of further concerns over security for the Beijing Olympics, this includes cyber crime, corruption, fugitive matters, intellectual property, human smuggling, repatriation and mutual legal assistance.

The Chinese organisers have responded to the particular challenges for Beijing security by exploiting techniques that further blur the boundaries between digital and physical security. In addition to the video surveillance networks, mentioned above, the organisers are deploying Radio Frequency Identification (RFID) systems. These are being integrated with building access control mechanisms so that signals from security devices will be wirelessly

transmitted to access check points. Electronic tickets with RFID tags can also help to monitor the holders' movements well before they reach the venue. This technology has also been integrated into a diverse range of logistics, such as the athletes' luggage, which might have security implications. All food entering the Olympic village will have a digital food safety logistics code and will be tracked using a combination of RFID and GPS technologies.

Conclusions and Further Work

This paper has described how the distinction between digital and physical security is increasingly blurred for Olympic events. In the past, computer networks were used primarily to store results for events and to coordinate the logistic information. However, the Athens games began to use digital infrastructures to carry images from surveillance cameras using the MPEG4 format across ATM switches. The Beijing Olympics will use sophisticated monitoring algorithms to introduce new levels of pattern detection into similar monitoring systems. There are also plans to use RFID tags and GPS applications to monitor diverse aspects of the games, including the physical movements of spectators and athletes. The intention behind these initiatives is to direct physical security teams against international and domestic threats that range from Islamic terrorism though to environmental protests. However, there are a number of concerns about the integrity of these systems. Previous physical attacks at Munich and Atlanta have shown the importance of preparing for contingencies including direct attacks on the security infrastructure. Problems with sub-contractors and claims of 'insider' threats against the Turin networks illustrate further threats to digital security. All of this must be placed in the context of increasing complexity both in terms of the Games themselves and in terms of the diverse computational systems that must be integrated into Olympic security applications. It remains to be seen whether or not the planning teams for Vancouver (2010) and London (2012) have learned the lessons that previous failures in physical security provide for the development of digital security at Olympic events.

References

C.W. Johnson, Using Evacuation Simulations to Ensure the Safety and Security of the 2012 Olympic Venues. In P. Swuste and A. Hale (Eds.) Proceedings of the 3rd International Conference Working on Safety, European Agency for Safety and Health at Work, Delft, Netherlands, 2006.

Biography

Chris. W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.