A Brief Overview of Technical and Organisational Security at Olympic Events

Chris. W. Johnson

Dept. of Computing Science, University of Glasgow, Glasgow, Scotland, UK, G12 8RZ.
Email: johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk/~johnson

Abstract. In July 2005, London was awarded the right to host the 2012 Olympic and Paralympic Games. The decision of the International Olympic Committee triggered considerable public enthusiasm across the UK. At the same time, it also created a host of logistical and technical challenges. Amongst these the first concern is to ensure the safety and security of competitors and of the public. This paper reviews the assets that are vulnerable to attack during Olympic events. These include spectators, participants, sponsors, Games infrastructure, the infrastructure of the host nation and security teams themselves. Later sections review the different threats against these assets, including malicious attacks from organized groups through to spontaneous actions by disaffected individuals. This analysis is based on a detailed survey of incidents at previous Games. The survey is also used to identify some of the constraints that affect security during the Olympics. It is difficult to apply risk-based approaches to guide the allocation of security resources. Further problems arise from the time constraints that all recent games have operated under. Delays in construction and funding together with the perceived need to use the most advanced technology combine to limit the time that is available to verify and validate security measures. Similarly, the increasing need to coordinate diverse national and international agencies can increase communications overheads and may lead to break down in passing on key intelligence prior to the Games. The closing sections address some of these problems. Computer simulation techniques can be used early in planning when there is some prospect of affecting the detailed layout of key sites. They can also be used closer to the Games, as training tools to rehearse key tactics and standard operating procedures before live drills can be conducted.

Keywords: Security, Olympic Games, London 2012, Infrastructure Security, IT Security, Computer Simulation.

1. Introduction

This paper describes the initial stages of a multi-disciplinary project that will model potential threats to security and safety during the 2012 Olympics and Paralympics. In order to understand these threats, it is first important to illustrate the scale of the Games. The security operation for the Athens Summer Games of 2004 had to protect more than 11,000 athletes who came from 201 National Olympic Committees and who participated in 296 events. The Games sold more than 3.2 million tickets; only Sydney sold more with 5 million in 2000. There were more than 21,500 media representatives in Athens. The US NBC network had more than 3,000 people. Media representatives were spread across 19 sports venues, 102 hotels and 7 media villages. The Games were broadcast to a worldwide television audience of up to 3.9 billion. Protecting these potential targets requires enormous resources. Athens was the most expensive Games costing approximately €9 billion ($11.6bn; £6.3bn). This was double the original estimate. The previous figures only include direct costs, they does not account for associated projects, such as a new airport and high-speed transit link to central Athens. €2.1bn was spent on the construction of sporting venues. Immediate infrastructure projects cost €2.8bn. Hospitality for the athletes and other variable costs came to €1.1bn. In contrast, security arrangements are estimated to have cost the Greek government more than €1bn. The net effect of these various commitments was that the national deficit rose to 5.3% of gross domestic product in 2004. The cost of securing the Games partly explains why the government violated the EC spending deficit cap of 3% of GDP.

1.1 What are the Assets?

The modern Olympic movement has been faced with a wide range of security threats. These include the more obvious forms of direct assault by well-organized terrorist groups. They also include spontaneous actions by disaffected or mentally disturbed individuals. The nature of these threats has changed over time. For example, recent Games have grown to depend on complex IT infrastructures. They are, therefore, more vulnerable to digital attack. In order to assess the risks associated with these different threats, it is important to consider the potential assets that might be the target of any attacks:

1. *Spectators.* The pipe bomb attack on the Centennial Park in Atlanta during the 1996 games illustrated the vulnerability not simply of the sporting venues but also of associated areas, including sponsors' exhibits, presentation areas, catering venues and so on. Although the Atlanta bombing was the work of a single, disaffected individual, the attacks of the 11th September 2001, as well as the bombings in Bali, London and Madrid have further heightened concern that terrorist groups might exploit media coverage of Olympic events by attempting mass attacks on the general public.

2. *Participants.* The Black September attacks on the 1972 Munich Summer Games completely altered the management of safety at Olympic events. It illustrated the vulnerability of competitors to determined and well organized terrorist groups. Inadequate preparations led to an ill planned and inflexible response as the authorities lost control of the situation. As we shall see, miscalculations about the number of attackers led to an insufficient number of snipers being deployed to prevent the terrorists' escape. This led to a prolonged exchange of gun fire that ultimately led to the deaths of the Israeli athletes and trainers.

3. *Flagship Events, Media Attention and the Kudos of the Games.* The Games attract massive public and media interest. They also have a growing reputation for their security measures. This increases the attraction for some individuals and groups to use flagship events as a vehicle for publicizing particular causes. For example, the Sydney games saw protests by Aboriginal groups. The Turin games saw a spectator run onto the ice during a curling match to advertise a gambling web site. These demonstrations often have peaceful intentions. However, there is considerable opportunity for an adverse outcome if, for example, security teams misread the level of threat.

4. *Sponsors.* Changing political, religious, economic and social movements have had an impact on the security threats that surround the Olympic Games. For example, some forms of mass protest have become less likely as popular governments have replaced the apartheid regime in South Africa. Conversely, the developing conflicts in Afghanistan, Iraq and on the West Bank have led to increasing concerns over suicide bombing. Recent games have also witnessed increasing levels of violence from anti-globalization protestors. In consequence, attacks have focused on the sponsors of the torch procession during both the 2000 Sydney Summer Games and the 2006 Turin Winter Olympics. Other attacks have focuses on commercial outlets including the Athens Olympic Shop, which was badly damaged during protests in 2004.

5. *Vulnerable Events.* Given the increasing levels of security at the principle venues, many demonstrations have now focused on other events that are associated with the Games. Protests marred both the Sydney and Turin torch processions. At the 2006 Winter Olympics, these demonstrations became violent. Demonstrators examined the routes to select crowded locations where these was little opportunity for successful intervention by security teams. The Marathon and long distance walking events are particularly 'vulnerable' for similar reasons. The Horen attack during the Athens Games will be discussed in later sections. However, the ease with which he was able to tackle one of the runners is illustrative of the potential threat for future events.

6. *Games Infrastructure.* There is growing concern about threats against the infrastructure that supports the Games. For instance, immediately before the 2006 Winter Olympics several terrorist groups were arrested for planning to attack the Metro system in neighboring cities. The Madrid bombings illustrate the potential for similar attacks on the public traveling to Olympic venues. It is also important to adopt an extremely broad definition of infrastructure targets associated with the Games. For example, information technology plays an increasingly important role across many different aspects of the Olympic organization. Not only do computer networks hold lists of participants, events and results. They also support the access control lists that are used to determine who can enter venues at particular times. The last three Games have also used relatively sophisticated computer networks to support the transmission and distribution of surveillance data through audio and video streaming. There have been reports of 'hacking' incidents at two previous competitions; these are described in greater detail in the following sections.

7. *Host Infrastructure.* Increasing levels of international cooperation, together with technological developments such as video surveillance databases have increased the level of protection available to the infrastructure of the Games. It, therefore, follows that potential threats may be directed towards 'softer' infrastructure targets, including embassies and government buildings. The sarin gas attack by members of the Aum Shinrikyo religious group on 20th March 1995 against subway trains passing through Tokyo's Kasumigaseki and Nagatacho provides a further warning of potential infrastructure attacks. The organizers of recent Games have, therefore, prepared to mitigate the effects of biochemical incidents. There has also been concern over the use of nuclear materials, especially following the arrest of a group from Afghanistan which possessed plans for the Lucas Heights reactor, before the Sydney Games.

8. *Co-located Events.* The Olympics is not simply a sporting event. Conferences and workshops for many different international groups take place close to the Olympic city in the knowledge that some participants will also attend the Games. These meetings can look vulnerable especially when national and international security resources are diverted towards the main venues. Co-located events often address topics that act as an independent focus for protest. For instance, there were violent clashes outside the World Economic Forum in Melbourne shortly before the 2000 Summer Games.

9. *Security teams.* The security surrounding the Games is also vulnerable to attack. Most obviously, there is a growing threat to the digital infrastructures when, for example, ATM switching is used to stream surveillance videos. However, terrorist groups have also launched attacks that are intended to probe the security of the games. For example, 'Revolutionary Struggle' bombed an Athens police station before the 2004 Olympics to point out perceived gaps in the security arrangements. The media have also launched increasingly sophisticated attempts to expose security flaws surrounding Olympic events. Although such investigative journalism can improve vigilance, it can also divert finite security resources.

This overview is incomplete; however, the following paragraphs provide a more detailed review of the threats against recent Olympics. They also introduce the organizational and technical measures that have been used to implement security policies at these events.

2. Previous Threats and Security Measures

In planning for the security of future Olympics, it is important to look back at recent games in order to identify potential threats. The following paragraphs look at deliberate attempts to breach the security surrounding the Games. In practice, organizers must consider a far broader range of incidents. These include fires that can be started inadvertently, as well as the structural collapses that have occurred during several previous sporting events. This decision is justified for the sake of brevity. However, many of the techniques that help to prepare for these intentional threats can also be used to plan for this wider class of security incidents.

Munich and the Terrorist Threat: The kidnap of eleven Israeli athletes and coaches from the Munich Olympic Village on the morning of 5th September 1972 provides a powerful example of what can go wrong. Although considerable controversy surrounds the planning and response of the German authorities, there is general agreement about the initial events. The attack was coordinated by a faction of the Palestine Liberation Organization known as the 'Black September' group. Five Arab terrorists climbed over a two meter fence wearing tracksuits with weapons hidden in athletics bags at 04:40. Two other members of the team used security credentials to join them inside the perimeter of the village. It has been claimed that these members of the group had been employed inside the Olympic village and had spent several days reconnoitering the area. The Palestinians used stolen keys to enter two apartments being used by the Israeli team. The wrestling coach, Moshe Weinberg, realized that something was wrong as he opened the door. He shouted a warning. Coach Tuvia Sokolovsky and the race-walker Shaul Ladany escaped. Four other athletes, two team doctors and the delegation-head managed to hide in the confusion. Weinburg and the weightlifter Joseph Romano, attempted to delay the terrorists. This allowed another athlete, Gad Tsobari, to escape. However, both Weinberg and Romano were killed. The terrorists then rounded up nine Israeli hostages. The Uruguay and Hong Kong Olympic teams shared the same building with the Israelis but were released unharmed. By 09:30, the terrorists had announced that they were Palestinians. They went on to demand the release of 234 Arab prisoners from Israeli jails. They also asked for the release of Andreas Baader and Ulrike Meinhof, who were members of the Red Army Faction held in a Frankfurt prison.

At 15:50, the decision was taken to suspend the games. During this time various plans were developed by the German authorities in order to free the hostages. A political decision was made not to accept an immediate offer of assistance from Israeli Special Forces even though it was subsequently claimed that many of the security teams who were used by the Germans lacked specialist training in anti-terrorist operations. By 17:00 it became clear that there was no immediate prospect of storming the building without harming the hostages. German police had been deployed around the building dressed in tracksuits. The media soon identified their positions. Members of the terrorist group could be seen leaning out of the apartment building to observe teams whose location had been shown in television coverage. Any plan for an immediate attack on the building was postponed when the terrorists threatened to kill two of the hostages unless the Police units withdrew.

The terrorists had demanded safe passage out of Germany. In consequence, attention began to focus on a rescue attempt while the group was in transit. German snipers were ordered to deploy to the NATO air base at Firstenfeldbruck. An agreement was reached between the German authorities and the Palestinians to transfer the hostages and terrorists to a plane destined for Cairo. Buses were used to take the group from the Athletes' village and at 22:10 the group boarded two helicopters to begin the transfer to what they believed was Riem airport. The helicopters landed at 22:30. An initial plan had focused on the use

of five or six armed police officers who were dressed as attendants on a decoy plane. These officers would overwhelm any terrorists who inspected the aircraft while the sniper teams fired on those who remained with the hostages. However, the team on the plane had little or no training in these operations and voted to abort the mission without reference to the control group just after the helicopters landed.

Four helicopter pilots and six kidnappers came down onto the tarmac. Two of the terrorists inspected the aircraft while their colleagues guarded the aircrews. When they discovered that the plane was empty, the terrorists began to run back to the helicopters and at 23:00 the marksmen were told to open fire. These snipers were selected for their marksmanship. However, they had little or no experience of hostage situations. They were not provided with radio communication equipment and had no means of coordinating their fire. They lacked protective equipment and were poorly sighted so that at least one sniper was wounded by a fellow police officer. They lacked night vision equipment and their rifles did not possess telescopic sites. In consequence, the authorities rapidly lost control of the situation. Two of the kidnappers holding the helicopter crews were killed and another was fatally wounded. The pilots began to run for safety, however, the hostages were still tied up in the helicopters and could not escape. The terrorists tried to shoot out the airport lights, killing a policeman in the control tower.

The authorities had not initially ordered any armored support and the fighting reached deadlock. It was after midnight before personnel carriers arrived, having been delayed by traffic on the approach to the airport. Around 00:04, one of the terrorists began to kill the hostages first by shooting at close range and then by throwing a hand grenade into the cockpit of the helicopter. Two terrorists attempted to escape on foot and were killed by the police. The remaining hostages were then either killed by police snipers or by one of the kidnappers. Three of the remaining terrorists lay on the ground and were captured by the police. The final terrorist was tracked using dogs and shot shortly before 01:30. It has been claimed that the plan was doomed to fail because the authorities had under-estimated the number of terrorists. They had planned for five rather than eight militants. In consequence, there were less sniper teams than would have been needed for simultaneous shots to be fired on all of the militants even if they had a perfect line of sight. Such criticisms ignore the basic logistical problems of coordinating such an attack. They also ignore the initial plan to incapacitate some of the terrorists using the agents who were disguised as cabin crew on the decoy plane.

These 1972 attacks persuaded the hosts of the 1976 Montreal games to reconsider the staffing and layout of their venues. The additional security arrangements together with some financial mismanagement and stadium costs raised the estimated expenditure from $310 to more than $1.5 billion. This, in turn, persuaded Colorado residents to vote against hosting the 1976 Winter Olympics after they had been awarded to Denver. The Colorado vote shows that escalating security costs can dissuade potential hosts from holding the games. There is always a conflict between the need to protect athletes and the public whilst continuing to ensure the future viability of the Olympic movement.

The impact of the Munich attacks continued to affect the Olympics during the 1980s. Organizers' focused on the potential threat from organized terrorism following the model provided by Black September. These concerns were justified by continuing political controversy over the Middle East and the apartheid regime in South Africa following their expulsion from the Innsbruck Winter Games in 1964. The USA led a boycott of the 1980 Moscow Summer games. Conversely, the Soviet Union cited security concerns as the primary reason for its boycott with 14 other countries of the 1984 Los Angeles Olympics. These concerns faded during the late 1980's. The Seoul summer games of 1988 were the first since 1972 without any major political boycotts. The winter games at Albertville and the 1992 Summer Olympics in Barcelona saw further relaxation following the break-up of the Soviet Union and the formation of a united Germany.

The Atlanta Bombing and the Threat from Disaffected Individuals: It can be argued that security vulnerabilities emerged because organizers' became preoccupied with the Munich tragedy. There is a natural tendency to guard against the last major attack rather than future threats. In other words, Olympic security focussed on organised groups from areas such as the Middle East rather than domestic threats from the host nation. However, such criticisms are too simplistic. Although the CIA supported the preparations for the 1996 Atlanta Olympics, for example by attempting to penetrate Hezbollah, it was the FBI who led the joint security programme. This ensured that considerable resources were focused on the threat from domestic groups as well as those from politically sensitive areas overseas. It was against this background that a pipe bomb was detonated in the Atlanta Centennial Olympic Park killing one person and injuring 111. The park was used to host corporate venues, concert stages and exhibits would reopen. This event forms a strong contrast with Munich. The 1972 attack focused on a small number of athletes from a particular nation while the 1996 bomb affected a mass group of spectators. The 1972 attack was orchestrated by a relatively well organised group of political activists with considerable financial and technical backing. The Atlanta bomb was planted by an individual whose motives were difficult to determine even after he issued the following explanation:

> "In the summer of 1996, the world converged upon Atlanta for the Olympic Games. Under the protection and auspices of the regime in Washington millions of people came to celebrate the ideals of global socialism. Multinational corporations spent billions of dollars, and Washington organized an army of security to protect these best of all games…the purpose of the attack on 27 July was to confound, anger and embarrass the Washington government in the eyes of the world for its abominable sanctioning of abortion on demand. The plan was to force the cancellation of the Games, or at least create a state of insecurity to empty the streets around the venues and thereby eat into the vast amounts of money invested".

From the perspective of the security teams, the incident began at 00:58 when a security guard, Richard Jewell, noticed an unattended green rucksack underneath a bench in the Centennial Park. He alerted a bomb disposal team and spoke with Tom Davis, a Georgia Bureau of Investigation agent, who was in the park on a routine call to disperse party-goers. Davis began to clear people away from the immediate area. At 01:07, a 911 caller stated:

Male voice: "There is a bomb in Centennial Park, You have 30 minutes."

The 911 operator then attempted to locate the address for the park so that they could complete a dispatch request for police teams using the 911 computer system. The operator found that the Police Department's Agency Command Center telephones were all busy and so she called the Zone 5 police precinct which included the Centennial Park. The subsequent enquiry published the transcript of the call:

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'?"

After the operator had checked their spelling of the name, they again tried to contact the Police Agency Command Center. As before, they initially could not establish a connection and were only able to get through on the third attempt. However, when she requested the location of the park, the 911 operator was given a further phone number:

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."

The 911 operator called the telephone number that she was given but was then put on hold for two minutes after asking for the street address of the Park. She mentioned the bomb threat to a supervisor while she was waiting for someone else to get the

address. The supervisor realized the seriousness of the situation and helped to provide the missing information. The initial bomb warning was received at 00:58. The 911 operator eventually sent the computer message to the dispatcher at 01:08. The dispatcher finally contacted a police unit at 01:11. Meanwhile, several officers at the park tried to keep the crowd away from the bag. At 01:08, the decision was taken to initiate an evacuation. Officers later reported that they were reluctant to broadcast a bomb warning in case it led to a panic amongst the people in the Park. This was a significant concern; the evacuation had to be conducted in the early hours of the morning with a crowd that had been enjoying the Olympic hospitality. A police unit reported an explosion in the Park at 01:20. The Atlanta hospitals had rehearsed their emergency response and began to deal with the 110 injuries. At the same time, police units acted to seal off downtown Atlanta in the hope of identifying the perpetrator. While the casualties and other members of the public were being evacuated, security teams searched for secondary devices and helped to safeguard the site for the subsequent investigation. As soon as these tasks had been completed, Olympic officials reaffirmed their intention that the games should continue. Security teams then 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 similar attack. Policies 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.

More than 100 reports of suspicious packages were made in the 24 hours following the explosion in Centennial Park. All proved to be harmless but these incidents placed immense stress on the police and other security agencies. The paradoxical effect of increasing public awareness was that the sheer number of false alarms may have created opportunities for subsequent malicious acts. It is important not to underestimate the impact of these calls. For instance, one report led to the closure of the 'Underground Atlanta' shopping mall. Thousands of people had to be evacuated during the evening following the bombing. Although the subsequent search lasted less than an hour, the evacuation caused considerable traffic problems. The mall was adjacent to the Five Points interconnection for Atlanta's MARTA rapid transit system. Thousands more people were affected when this main north-south and east-west transfer point was closed. The package turned out to be a clothes iron. One week after the bombing, the Centennial Park again had to be evacuated in response to a 'suspect package'. Security teams were able to reassure visitors and quickly reopened the park. However, each successive evacuation placed further strain on finite security resources.

Subsequent investigations focused on whether the location of the Park should have been better integrated into the computer dispatch system. Atlanta, therefore, provided 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. The Atlanta bombing also provides a further illustration of the level of detail that must be addressed in security plans. Teams must look beyond the confines of the Olympic park to consider whether emergency services can provide necessary support in a timely fashion. Suspicion initially focused on the security guard, Richard Jewell. However, he was subsequently cleared of any involvement. Attorney General Janet Reno publicly apologized for his treatment. Considerable public and political criticism was then directed towards the handling of the case before the right-wing extremist Eric Robert Rudolph was arrested. In the meantime, he went on to perpetrate three further bombings.

Sydney the Threats of Mass Public Protest and Weapons of Mass Destruction: The Atlanta bombing demonstrated that massive security investments cannot guarantee the safety of the public. It also prompted a 'root and branch' review of security for the Sydney Olympics in 2000. Preparations were made for potential attacks from organized terrorist groups, based on the events at Munich in 1972. Special Air Service soldiers, navy divers and a Black Hawk helicopter squadron spent 18 months training for these threats. Other arrangements were more directly focused on a potential recurrence of the Atlanta bombing; "The real danger will come, rather than from some huge well financed, well resourced terrorist group ... (but) from the individual nutter making a bomb in the basement or garage" (Reuters, 2000). In addition to the bag checks and metal detector cordons, 20,000 soldiers, reservists, police officers and volunteer security officials were recruited. In spite of these preparations, organizers and government officials continued to recognize their vulnerability. These concerns did not simply center on organized terrorist groups and individual bombers. They were also concerned about the security implications of large-scale, public protests. Before the games, there were sustained clashes between Australian police and anti-capitalist demonstrators in Melbourne. Civil rights campaigners argued that these demonstrations were met with a deliberate show of force that was intended to deter anyone who might disrupt the Olympic events.

Further concerns focused on the use of nuclear and biological agents. These fears stemmed from international political instability. Relationships between Iraq and several Western nations continued to be strained following the 1991 Gulf war. There had also been a series of explosions at US embassies in Africa during 1998 and there were fears over terrorist attacks backed by the Taliban in Afghanistan. The Sydney organizers were also worried that an attack using sarin gas against passengers on the Tokyo underground during March 1995, might provide a template for an attack on the Games. Their

concerns seemed to have been justified when 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 BBC (2000) account of these arrests observed that "they have suspected links to Osama Bin Laden, the Saudi millionaire considered by the Americans to be the world's most wanted terrorist".

Salt Lake City and the Changing Climate After 11th September, 2001: The use of commercial aircraft against large public buildings on 11th September 2001 forced the organizers of sporting events to consider a range of hazards that previously were considered to be very unlikely. The impact of 9/11 can be illustrated by comparing Salt Lake City in 2002 with the last winter games to be held in the United States at Lake Placid in 1980. The total budget at the previous games was $168 million. In 2002, the Winter Olympics cost more than $2 billion. Around 1,000 security staff were recruited for Lake Placid. At Salt Lake City this had reached 10,000. The security budget for Salt Lake City was around $300 million; over 12 times more than the security budget for Lake Placid. However, the 2001 terrorist attacks did not 'revolutionize' Olympic security. Instead, they provided a catalyst for changes that were already underway. The Sydney 2000 games had seen significant increases in the scale and complexity of security arrangements. Salt Lake City was the first Games to be declared a US National Special Security Event. However, this was announced in 1999 well before the attacks on the World Trade Centre, the Pentagon and Flight 93.

The US Secret Service acted under the Department of the Treasury to design, plan and implement security for the 2002 Winter Games. In addition, state and local law enforcement agencies coordinated initial planning through the Utah Olympic Public Safety Command. During the Games, these agencies ran security operations through an Olympic Coordination Center (OCC). In addition, a Joint Information Center was established in the State Capitol Building to provide a 'one stop shop' for public safety information. Such coordinating initiatives were essential given the number of agencies that were involved in securing the 2002 winter games. 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 (FEMA) 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 to be 'on call' during the games. 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 provided over 100 deputies to as security backup for Public Health Service emergency medical teams. The Bureau of Alcohol, Tobacco and Firearms assisted the FBI in detecting and responding to any incidents involving explosives or where arson was suspected. The Department of Energy monitored energy infrastructure provision and organized nuclear response teams. The Environmental Protection Agency provided state and local teams to deal with any potential hazardous materials in coordination with teams from the Department of Health and Human Services. This agency provided 18 medical strike teams, and a 36-person National Medical Response Team. The Centers for Disease Control provided emergency response coordinators, lab scientists and other professionals to support these teams from Health and Human Services. The Food and Drug Administration conducted food safety inspections at Olympic venues, including the athletes' village. Over 100 Forest Service officers were deployed on the slopes and mountain perimeters. The National Park Service monitored outdoor venues for events including downhill and cross-country skiing as well as bobsledding. The Department of Transportation was responsible for supporting any evacuation from the Salt Lake City area in response to an incident. They were also to help transport response teams and equipment should they be needed (White House, 2002).

These details illustrate the range of resources that are deployed to secure the Olympic Games. They also provide some impression of the logistics that must be addressed by the organizing committees of major sporting events. The planning and preparation for inter-agency coordination were tested through drills and exercises in the months leading up the Salt Lake City Games. For example, a Command Post Exercise was conducted by the FBI and the Utah Olympic Public Safety Command during November 2000. This exercise was to determine whether various agencies could use the new communications infrastructure under a simulated emergency. A Field Training Exercise was also held 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. Other exercises were more specialized. For example, the Department of Defense's Defense Threat Reduction Agency supported the release of sulphur hexafluoride, a non-toxic, inert tracer, over Salt Lake City. Monitoring equipment was then used to track the tracer as it dispersed with changes in wind pattern, temperature profiles and moisture at different levels in the atmosphere. This information was to be used in the aftermath of a nuclear, chemical or biological attack.

Not only did these exercises provide important operational information, they also addressed public concerns in the aftermath of 9/11. Following these attacks, the Salt Lake City organisers added $34.5 million to a security budget of more than $300

million. This helped to fund more than 7,000 security personnel, including federal, state, military and private staff. Plain clothes officers mingled with the crowds. Portable X-ray devices scanned suspicious mail packages. Rucksacks and large bags were banned from all Olympic sites. Biometric scanners were used to identify athletes and officials. Vehicles were prohibited from approaching within 300 feet of the venues and other designated buildings.

Athens and Insurance: International events fuelled concerns over potential threats to the Olympics between Salt Lake City (February 2002) and the Athens Games (August 2004). The invasion of Afghanistan began during October 2001, however, operations continued throughout this time as coalition forces hunted for Taliban and Al-Qaeda insurgents. The Moscow theatre hostage crisis started on the 23rd October 2002. 42 Chechen terrorists seized 900 hostages inside a theatre. All of the terrorists and 130 of the hostages died when Spetsnaz used a chemical agent against the occupants. The second invasion of Iraq began during March 2003 and led to widespread protests among both nation states and dissident groups. Tensions continued in response to the al-Aqsa or second Intifada, which began in September 2000 and continued until the Sharm el-Sheikh Summit of 2005. There were bomb attacks on crowds in an entertainment district in Bali (12th October 2002) and on crowded commuter trains in Madrid (11th March 2004). Concerns over Olympic security were justified when the 'Revolutionary Struggle' terrorist group used explosives to destroy an Athens police station during the night of 5th May 2004. Nobody was injured. 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 national and international events led the International Olympic Committee for the first time to insure against the partial or full cancellation of the Games. The £93 million policy covered terrorism, earthquakes, flooding and landslides.

The opening sections of this paper have described the financial demands that were placed on the Greek national economy by the 2004 Olympics. Security operations cost €1 billion, and represented more than 10% of the total direct costs. The expenditure on securing the Athens games was almost four times greater than for Sydney in 2000. 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. These trends raise important questions for future Games. Beijing (2008) can call on a state infrastructure that is not available to London (2012). However, both 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.

Organisational Complexity: 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 (OGSD) reporting to the Chief of Police. The OGSD included members from the Police, Coast Guard, Fire-Brigade and Defence Forces. This unit helped to exchange operational information during the planning and running of the Games. It filled a role that was broadly similar to the Utah Olympic Public Safety Command at Salt Lake City. The OGSD also helped to operate an Olympic Intelligence Centre (OIC). 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. Hence it performed some of the functions associated with Utah's Olympic Coordination Center and the Joint Information Center from Salt Lake City.

The geography of the 2004 summer games also implied greater cooperation between the local organizers and international agencies. NATO assisted with sea and air patrols. In particular, they provided Airborne Warning and Control System aircraft. A Patriot missile battery was placed near Tatoi airfield, close to the Olympic village. Russian-made S300 anti-aircraft missiles protected Heraklion and other host cities. The Greek government also received support from the International Atomic Energy Agency (IAEA) in detecting and deterring a potential dirty bomb attack. The IAEA provided both fixed and portable radiation detectors for several of the Olympic venues and at major border crossings. An Olympic Security Advisory Group was established to share information and expertise between Australia, France, Germany, Israel, Spain, US and UK. Members of the FBI and Scotland Yard advised on anti-terrorism issues. The Israelis provided specific training on how to reduce the threat from suicide bombers. The initial risk assessments conducted by these international, inter-disciplinary teams focused on the threats to athletes and officials from the USA, UK and Israel. Guards traveled on their buses with close support from police helicopters. Athletes from countries involved in the Iraq coalition received similar protection.

Technological Infrastructures: A significant proportion of the security budget funded a dedicated information network. This helped to merge thousands of streams of continuous video, audio and data from 63 command centres with 1250 operators, monitoring 47 venues over an area of 250 square kilometres. Technical solutions involved MPEG4 digital surveillance cameras using video over the Internet Protocol (IP) with Asynchronous Transfer Mode (ATM) switching. In some locations, however, existing analogue cameras were also 'patched' into the digital network. Operators can also use the speakers attached to surveillance cameras to make crowd control announcements. This digital architecture offered considerable advantages. For example, access control software tailored the privileges associated with different operators to their individual requirements.

This functionality was important given that multiple agencies including the Police, Coast Guard and Military could draw feeds from the system. 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 Athens network was one of largest video-IP networks to be developed by the time that the Games started. The technical innovation and scale of the command and control systems led to considerable delays. This limited the use of the systems during the exercises that were used to test other aspects of security.

Just as Salt Lake City held Command Post and Field Training Exercises, the Athens OGSD held seven major drills before the Games. Major security exercises took place in early February and mid-March in preparation for the opening in August 2004. They involved all of the agencies involved in the OGSD and were designed to test both operational effectiveness and the agencies' ability to respond to changing events. These exercises lasted more than two weeks and involved 1,500 of the local security personnel with the participation of several hundred US soldiers. They were observed by the international experts from the Olympic Security Advisory Group. As in Utah, considerable attention was paid towards detecting and dealing with weapons of mass destruction. For example, the drills held in March 2004 focused on a simulated chemical attack, a plane hijacking and an epidemic outbreak. However, there were several criticisms of the security preparations for the Athens Olympics. The Greek organizing committee had planned for 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 the continued US participation (BBC, 2004).

The Role of Media: Like many previous Games, security arrangements were subject to considerable media scrutiny. Journalists went to elaborate lengths to 'test' precautions. For example, the UK Sunday Mirror newspaper ran a story in which an undercover reporter was supposedly offered employment within the main stadium without an adequate vetting procedure. He allegedly provided a false name, was not asked for references and did not have a formal interview. The story alleged that that reporter worked there until the opening ceremony and during this time was able to plant a number of bogus packages. These included mock bombs constructed from plastic materials, wire connectors and batteries. These remained hidden after several security sweeps including a 'lock down' on the 5th August. The reporter was also able to get close to a number of VIP's including the British Prime Minister. The Greek Public Order Minister George Voulgarakis argued that the story was a "profound insult to journalism and the principles of objective and responsible reporting" (Associated Press, 2003). The meta-level point here is that investigative journalists will continue to probe the effectiveness of security arrangements in future games. The increasing security budgets and the need to reassure the public combine to fuel media interest in identify security problems. However, as we have seen, it is impossible to completely guarantee the security of such a large and complex event. It remains likely that journalists may identify apparent problems even if, in practice, those problems could not have provided a pragmatic opportunity for terrorist attacks. It is, therefore, critical that organising committees learn from similar journalistic enterprises. In particular, security teams must act to rectify genuine vulnerabilities. It also seems appropriate to prepare counter-briefings in order to reassure the public and participants.

Olympic Security teams face conflicting requirements. Not only did the media criticize apparent security lapses at the Athens Olympics but they also criticized the high-levels of security coverage. The Sunday Mirror article can be contrasted with a piece from the Washington Post (2004) entitled 'Extraordinary lengths taken to protect Olympics'. Another article cited a US hurdler; "Every step you take, there are guards with machine guns in the Olympic Village, I know they're there to protect you, but it's scary. I'm not used to it, so it makes me cringe a little bit. It wasn't like this at all in Sydney" (San Francisco Chronicle, 2004). They went on to complain about the concrete and steel barriers that protected the US Embassy and the Olympic Hotel where many officials were based. Further press criticism focused on access to some venues. The Chronicle reporter describes how he had to approach two local officials and five police officers before he could look at the rapids in the whitewater kayak venue. Local organizers provided a measured response to these criticisms. Gianna Angelopoulos-Daskalaki, head of the Athens Organizing Committee stated that it was not possible to provide "absolute security" without hampering athletes, officials and spectators; "our strategic decision, from the first minute, was to highlight the celebratory character of the games and not have them look like a military zone" (Associated Press, 2003).

Vulnerable Events and the Individual Maverick: The Athens games again illustrate the difficulty of providing protection against individual protestors during vulnerable events. For the summer games, long distance walking and running competitions create huge logistical problems as athletes compete across public roads. Long-distance skiing disciplines create similar problems for Winter events. In 2004, Vanderlei Cordeiro de Lima was tackled by a former Irish priest Cornelius "Neil" Horan while he was leading the marathon. The protestor had a piece of paper attached to his back bearing the message: "The Grand Prix Priest Israel Fulfillment of Prophecy Says the Bible". The runner was held to the ground for several seconds before rejoining the race. De Lima eventually completed the remaining three miles and finished in third place. His subsequent appeal to be awarded the gold medal was turned down, however, he received the Pierre de Coubertin Medal for 'fair play'. After the event, the president of the Brazilian Olympic Committee criticised the security measures stating that the lead runner should always be

flanked by at least two motorcycles. However, such measures seem unlikely to eliminate all potential threats. There are several worrying aspects of the Horan attack. The former priest had a previous history of disrupting major sporting events. He had made previous attempts to demonstrate on Wimbledon's center court during a rain break, and had tried to disrupt cricket and rugby matches. Most notably, he ran onto the track during the British Grand Prix forcing cars to swerve around him at racing speeds. It is unclear whether any risk assessment had considered Horan's previous behavior or whether such an assessment was made available to the Greek officials through the OGSD. Horan was given a one-year suspended sentence and was fined $3,600; an arguably lenient sentence given the potential seriousness of the incident.

Militant Islam and the Turin Winter Games: The security teams for the 2006 Winter Olympics in Turin had to face potential terrorist threats both from inside Italy and from external sources. For example, wire-tap evidence and a Tunisian informer led to the arrest to 3 North Africans for planning to bomb part of the Milan Metro in February 2004. This group was linked to a Mosque in Cremona whose former imam, Tunisian Mourad Trabelsi, had already been arrested. 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. All five were connected to the Islamic Cultural Institute in Milan. There were strong similarities between these various groups and those involved in the London bombings of 7th July 2005. The London attacks again illustrated the vulnerability of mass transit systems to well organized, suicide attacks. Partly in response, the Italian government reformed its anti-terrorism laws. It also initiated a range of intelligence activities in Turin's 100,000 strong Muslim communities. These initiatives faced the considerable problems of identifying whether individuals had explicit links with al-Qaida or the Mujaheddin Council. The London bombings also showed that the absence of such links did not preclude involvement in militant actions. Government concerns were further fuelled by messages from Ayman al-Zawahri on 1st September and Adam Gadahn on 11th September 2005 threatening attacks on Europe in the immediate future. Later that month, the Italian courts acted to expel one of Turin's imams, Bourki Bouchta, for links to a Morrocan Islamist Combat Group know as GICM. He was arrested under the legal reforms, mentioned above, and was immediately placed on a plane to Morocco even though he had lived in Italy for 19 years. Tensions increased following the publication by the Danish newspaper Jyllands-Posten of cartoons depicting the prophet Muhammad on 30th September 2005. Initial protests by Danish Muslim groups led to more violent demonstrations especially in the Middle East.

Globalization: The organizers of the 2006 Winter Olympics were also concerned about local protests following the violence that was targeted against the G-8 summit in Genoa during July 2001. In particular, security teams had to consider the threat posed by the Italian anarchist movement. Groups, such as the Informal Anarchists Federation (FAI), sought to promote anti-capitalist and pro-environmental policies. This led them into conflict with many aspects of the modern Olympic movement. In particular, complaints focused on sponsorship by major corporations and formed part of a wider series of attacks in Italy on McDonalds, Blockbuster and other US franchises. The Games organizers' concerns were further heightened by a series of attacks on national and regional infrastructure projects, corporate offices, and Italian government buildings. There were up to 60 of these incidents during 2005, most involved improvised explosives and were intended to raise publicity without causing injury.

Environmental Protests: The continuing threat post by anarchists groups fed into wider concerns and mass protest against a new high-speed railway line known as the TAV (Treno ad Alta Velocità). More than 50,000 people joined a march against the TAV in the Val di Susa near the Italy-France border. Local residents and environmentalists complained about the environmental impact and 'unnecessary' expense of a rail tunnel which was to be blasted through the Alps. Initial demonstrations were peaceful, however, they quickly led to clashes. On the 6th 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. These events illustrated a convergence of mass protest and more militant political groups, such as the anarchist groups mentioned above. These links may, in turn, explain the relatively tough measures taken by the Italian Interior Ministry against the protestors in the Val di Susa. Although there were no explicit links between the TAV and the Turin Olympics, many of the groups involved in actions against the railway also criticized expenditure linked to the Games. The U.S. State Department's Overseas Security Assistance Council noted: "Several activists have linked the TAV construction project with the infrastructure development for the 2006 Winter Olympic Games due to the perceived similarities in harming the environment and disruption to local communities in Turin and surrounding areas" (NBC, 2006).

Protests against the TAV and the Olympics came together in more than 30 demonstrations along the route of the Olympic flame. The torch symbolizes peace and friendship amongst the competing nations. However, an Alberta native group had demonstrating on the route of the torch relay to publicize a land dispute with the Canadian government before the 1988 Calgary games. Several aboriginal groups had also marked many of the stages of the route to Sydney in 2000. In 2006, the torch acted as a focus for diverse protest groups ranging from Campaigners for a Free Tibet to Anti-Globalisation demonstrators. This latter group had protested against the relay since the introduction of corporate sponsors in 1983. Carrying the Olympic flame across the host country is an Olympic tradition that, like the marathon, provides links between the modern

movement and sites associated with the ancient games. Also like the marathon, the torch procession creates huge challenges for security teams. On the 5th February 2006, TAV protestors in the town of Susa briefly covered the torch with a flag in an attempt to either burn it or to extinguish the flame. More than 1,000 people formed a crowd in which demonstrators were mixed with family groups on a narrow bridge The runner managed to force their way through and police arrested the protestor. The procession was then diverted from its intended route through the Val di Susa towns of Bussoleno and Borgone Susa. The police cited 'public order concerns' but the organizers than had to insert an additional stage between Oulx and Bardonecchia to accommodate all of the runners who might otherwise have lost their turn carrying the torch. Several hundred protestors carried out their demonstration in Bussoleno despite the absence of the torch. They were able to use a genuine torch that had been stolen during a previous demonstration.

The final accounts for the Turin Games have still to be published; however, the security budget is estimated to have been more than $250 million. This is less than one quarter of the amount spent on the Athens games. However, the organisers argued that they were able to reduce the costs by using the existing security infrastructure. The winter games are smaller in scale and many mountain venues are physically easier to secure than their counterparts in the summer Olympics. An initial bomb-sweep was made across many of the venues in January 2006. Most of the sites were 'locked down' from 2nd February in preparation for the Games, which ran from 10th to the 26th February. Higher levels of security were associated with competition venues and the athlete's village compared with the sites for Olympic concerts, medal ceremonies and sponsor events. These non-competition venues included the Piazza Castello where medal ceremonies were staged every night at 20:00. They also included the sponsors' area on the Piazza Solforino. The previous attacks on the Olympic torch justified slightly increased levels of protection given the corporate involvement in this area. Hence, Piazza Solforino became a 'pedestrian only' area with a protective perimeter including compulsory searches. The NBC media centre and a refreshment complex in the Piazza San Carlo was protected by covert surveillance and was not protected by a formal perimeter. This decision may have been in response to media complaints against security measures at both the Athens and Sydney Games. For higher priority sites, the safety policy focused on concentric rings with increasing precautions being taken as visitors, officials and competitors approached the competition venues, housing and broadcast areas. For the competition venues, the outer rings included a stand-off zone at 100 meters to provide protection against car bombs. Only vehicles registered on the security central database could enter this zone. Such vehicle permits were restricted to employees, athletes, media and security officers. All vehicles were inspected except for VIP's arriving with a police escort. There were obligatory bags searches for everyone entering the venues and metal detectors were used. Dog teams also searched the crowds for explosives. The organizers attempted to provide separate physical entries for the media, athletes, spectators and VIPs. Spectators were told to allow two hours in order to enter most venues and up to three hours for mountain events.

The physical security measures for the 2006 Winter Olympics included 15,000 Italian federal, state and municipal law enforcement personnel. There were more than 10,000 police and 2,500 soldiers on duty during the Games. 300 snipers were deployed on the sloped around the main venues. 40 soldiers were assigned to emergency snowmobile vehicles. Fire crews with specialist training in nuclear, biological and chemical attacks were also deployed in Turin and near to the mountain venues. Military helicopters were used extensively for surveillance during the Alpine and cross country events. As in the Athens games, the Italian organizers recruited a range of specialist expertise from other countries to supplement their security provision. NATO sent two AWACS planes during the Games; these were used to implement a 'no-fly zone' during the opening ceremony. Liaison groups again coordinated the exchange of intelligence, 'lessons learned' and operational information with other countries. These included members from the Group of 8 (G8) countries, from European Union states and from 'high-risk' nations including Israel. Officers were sent from Europol and Interpol. The U.S. government established a dedicated security support office in Turin. They also set up a 24-hour Joint Olympic Fusion Center as part of the National Counter Terrorism Center in Virginia.

The 2006 winter Games were managed by a committee known as TOROC (Torino Organising Committee 20th Winter Olympic Games). They established a Safety and Security Committee and created a series of joint agreements with external agencies to identify responsibilities during the initial planning for the games. For example, a Memorandum of Understanding on the Security of the Torino 2006 Olympic and Paralympic Winter Games was created with the Turin prefect on behalf of the local police during July 2003. TOROC and its Safety and Security Committee were to assure safety in the work sites and jointly establish a security system with a Police planning group (Gruppo di Pianificazione della Prefettura). The organizing committee followed the policy of previous games by establishing the organization structure for security at a very early stage in the planning process. This joint Gruppo di Pianificazione della Prefettura considered the deployment of security devices such as surveillance cameras, metal detectors etc. It also helped to develop requirements for infrastructure provision and the security technology necessary to implement access control policies. Francesco Norante, head of the Safety and Security Committee argued that they were "perhaps the only Organising Committee that has given a lot of attention to defining the responsibility of the State and of the Committee regarding security for the event. The agreement has been a good working base, avoiding duplication and at the same time covering all areas" (TOROC, 2004).

During initial planning, TOROC's Security and Safety group employed about twenty people who were security experts or who had experience in managing large public events or who had specialist Police/Military expertise. 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 the TOROC organizers and external agencies including National Olympic Committees, the individual Sports Federations and the Sponsors. The third focused on security arrangements for competition venues. The fourth and final team focused on other 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. Norante again stressed the need to identify consensus between these different planning and operational groups "Right from the outset it was essential to work together with the Police, who have the mandate to plan the security for the entire event. Together we've identified concerns and searched for solutions. Without overstepping boundaries, we are succeeding in conveying the culture behind this great sporting event" (TOROC, 2004).

A range of companies provided the Turin games with a technological infrastructure that was similar to the digital networks behind the 2004 Summer Games. The IOC had previously selected Atos Origin as their 'Worldwide Information Technology Partner'. They were, therefore, responsible for managing data communication and providing a unified command infrastructure to the Turin organising committee. This company employed more than 2,000 people during the games to maintain the IT infrastructure. The complexity of these tasks stems in part from the multiple organisations involved and also from the technical requirements of 385 servers, 5,000 computers, 700 printers, 22,000 miles of cable, and 950 commentator information terminals. Over 100,000 person hours of testing were used to assess the security and reliability of the networks. They also used a wide range of standard operating procedures to protect their systems. For example, the 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 unauthorised device was connected to the network. The device was automatically disconnected. 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 and it is difficult to determine the seriousness of the threat (Associated Press, 2006). In addition to the digital attacks, mentioned above, a number of minor concerns were raised about the physical security of some venues:

> "At one media village hosting journalists in the north of Turin, two private guards checked credentials, but access was unrestricted at another less than a kilometer (half a mile) away. At the Oval, in the Lingotto area, a large section of a perimeter fence appeared unguarded Sunday, and one gate was left ajar though it was locked with a loose-fitting chain. Officers complained they had not received a promised winter uniform and had to stand guard in the cold with only a light jacket. Organizers for the Olympics also faced other last-minute challenges, with snow causing an unused security tent outside the Lingotto complex to collapse into a busy road Saturday" (Associated Press, 2006a)

These criticisms are similar to press concerns over the security at the 2004 summer games. The authors seem unaware that different levels of security were associated with different zones around key venues. They perhaps illustrate an expectation that security levels should be the same across all venues. Equally, however, they may also indicate vulnerabilities that persist in security provision in spite of the millions of Euros that have been spent in recent Games.

3. What are the Threats?

Figure 1 provides an overview of different dimensions of threat observed from recent Games. These range from single individuals, in the case of the Atlanta pipe bombing, through to the teams involved in the Black September attack and the Lucas Heights plans. The second dimension refers to the malevolence of any security threat. This is a more subjective scale.

However, it seems necessary to distinguish the level of threat posed by the Turin 2006 streaker from the 'Revolutionary Struggle' bombings before Athens 2004. This subjectivity makes it difficult to provide a definitive map. It is difficult to compare the relative malevolence of Sydney's World Economic Forum riots with Turin's anti-TAV demonstrations. However, Figure 1 does provide a broad overview of the security threats that have affected recent Olympics.

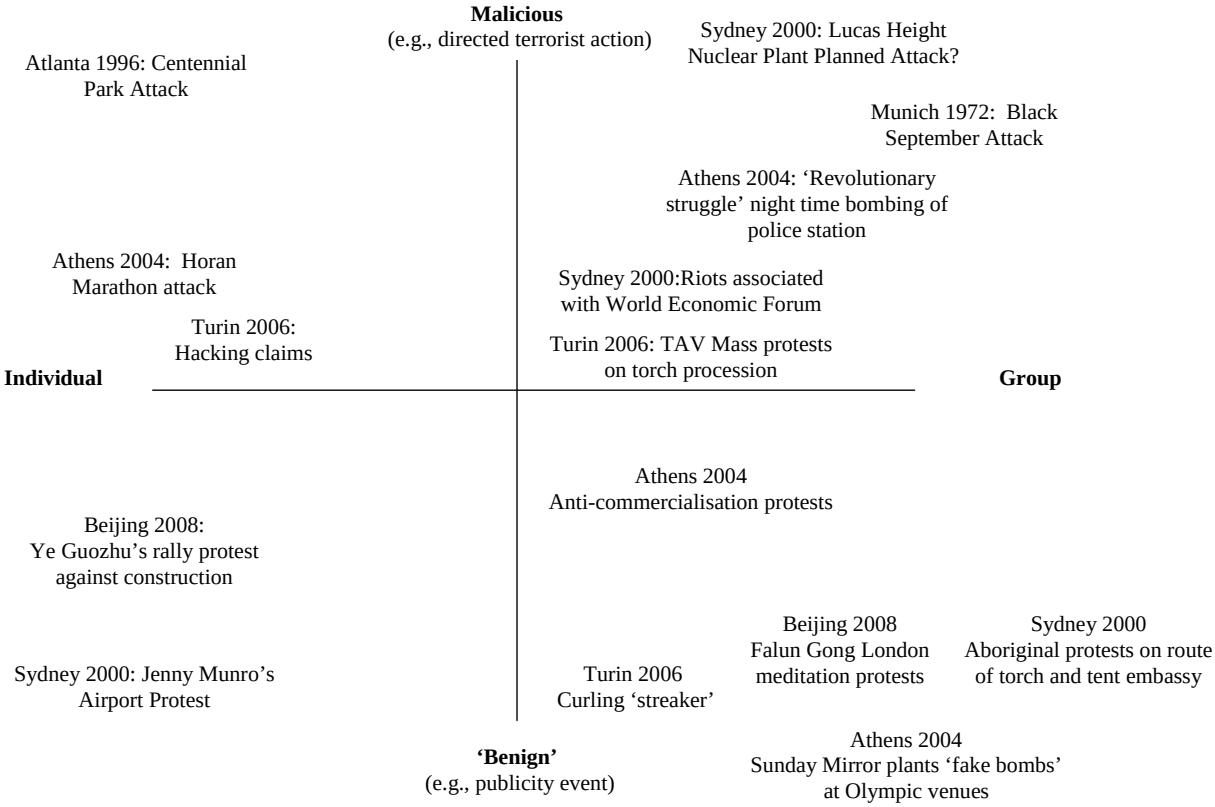

Figure 1: Dimensions of Olympic Security

1. *Group-Malicious Acts.* Images of the Black September attack on the 1972 Munich Olympics continue to have a powerful impact on the organizers of both winter and summer events. They have responded by fortifying key venues, by isolating the Olympic villages and by reorganizing the transport infrastructure to protect participants in transit. Governments have responded by monitoring and expelling known sympathizers before events are held. As we have seen, these measures often provoke considerable criticism. Protective measures isolate participants from the public, this alienates sponsors, spectators and the athletes. The media often attack any perceived erosion of civil liberties associated with sporting events. Police actions can particular provoke resentment when applied to mass protests rather than terrorist movements. Although these mass protests are, typically, benign in the sense that they do not deliberately set out to cause injury or loss of life they can quickly become violent as the 2006 protests in the Val di Susa have illustrated. The style of policing can have a considerable impact on the consequences of these events. Both the Italian and Australian security operations before the 2000 and 2006 games led to criticism of a 'heavy handed' approach that was intended to 'send a message' to potential mass demonstrators. Balanced against these criticisms, it is relatively easy to envisage other more malevolent forms of attack exploiting the confusion created by these mass demonstrations.

2. *Group-Benign Acts*. There are also more 'benign' forms of group security threats. For example, the Sydney 2000 Games provoked several protests over aboriginal rights. These included an 'embassy' of more than 100 tents, run by Isobell Coe in Victoria Park. She argued that "We're not a part of the protests, we're a peacekeeping camp, calling for an end to the genocidal 212-year war by white Australians against indigenous people" (Guardian, 2000). Similar peaceful events include the Falun Gong's meditation protests against the location of the Beijing 2008 games. Figure 1 also includes anti-sponsorship protests in this area of large-scale or organized threats that are 'benign'. This illustrates the subjectivity of our analysis. Similar riots have sparked violence when they merge with campaigns against globalization. The key point is, however, to demonstrate the range of different security concerns that arise both before and during any Games. For example, Figure 1 also includes the streaker who disrupted the 2006

curling match between the U.S.A. and Great Britain. This individual had an advert for an on-line gambling company drawn on his chest. The interruption occurred during the fifth-end break and was treated by both the players and the crowd as a relatively light-hearted incident. However, the individual was able to evade security and encroach the playing area. This incident can be placed in the Group-Benign quadrant because of his connections with the company that he advertised although it can be argued that he acted alone.

3. *Individual-Malicious Acts.* The pipe-bomb attack on the Centennial Park during the 1996 summer Games in Atlanta illustrates further threats against recent Olympics. It is difficult, if not impossible, to guard against the malicious actions of a single, determined individual. Security teams have responded by establishing perimeters around key assets. X-ray devices, portable metal detectors, explosive sensing animals are all increasingly being used to prevent this form of attack. In consequence, spectators must now arrive up to three hours before some Olympic events. As we have seen, complex IT systems must also be deployed to enforce access control during the Games. These systems help to prevent unauthorized access. However, they also create further potential vulnerabilities. Both Salt Lake City and Turin have suffered attacks on their IT infrastructure. Some of these attempts to break computer security have been perpetrated by 'insiders' with apparent grudges against event organizers. Further threats stem from individuals trying to use the forum provided by mass media coverage of Olympic events. The Horan attack during Athens 2004 arguably cost Vanderlei Cordeiro de Lima the Olympic marathon title during the Athens summer Olympics. Figure 1 distinguishes this event from the 'streaking' incident in 2006 because Horan deliberately attacked an athlete to bring attention to a particular cause whereas the streaker merely sought to advertise a service without attacking anyone. It is important not to underestimate the potential risks associated with actions like those of Horan in the Athens games. Many Olympic events carry an intrinsic level of risk that would be increased by any external intrusion. Horan's previous incursion onto the track of the British Grand Prix illustrates the potential threat from such individual acts. These individual acts also have the potential to escalate. A robust response from security forces could easily lead to loss of life.

4. *Individual-Benign Acts.* Individuals often use the media interest in the Olympics to highlight particular concerns in a manner that is not intended to threaten the safety of anyone connected with the Games. For example, Jenny Munro conducted a silent individual protest against the violation of aboriginal rights before the 2000 Sydney Olympics (Guardian, 2000). She spent several hours standing on the road between the airport and the Olympic venues. Her case like that of Ye Guozhu is interesting because they protesting against pre-existing problems that had been exacerbated by the preparations for the Olympics. In Sydney, aboriginal leaders protested against the manner in which new 'stop and search' powers, which were introduced to increase security for the games, seemed to unfairly target aboriginal young people. In Beijing, Guozhu's arrest followed protests against urban planning as part of 'urban regeneration' that had gathered pace in the run up to the 2008 Games. Although both of these security-related incidents are shown as individual protests, both Munro and Guozhu had hoped to generate wider support.

Although figure 1 provides a high-level framework for the classification of threats against the Olympics, it is important to stress that this taxonomy is constructed with the benefit of hindsight. It is security teams 'on the ground' who must make snap decisions about the malicious intent of any particular act. Attempts to connect a personal laptop onto a secure network may appear to be the benign 'mistake' of a single individual but it might equally be a precursor to a more coordinated, malicious attack. The following section explores these issues in more detail and identifies the pragmatic constraints that affect security teams in the weeks and months before the Games take place.

4. Compromises and Constraints

It is important to stress that we cannot provide complete protection against the threats listed above. Although organizers devote enormous budgets to protecting spectators and participants, there always remains a small but significant risk from disaffected individuals and determined groups with external support. Increasingly, also, delays in construction and planning place significant limits on the number and range of drills that security teams can perform to test the effectiveness of their plans before Games take place. The following paragraphs, therefore, summarize further constraints that must be considered when securing the Olympics:

1. *Limited budget versus infinite demands.* The opening paragraphs described how security consumes a significant proportion of the budget for any Olympic games. Adverse events ranging from the Munch and Atlanta attacks through to the Bali and Madrid bombings can be used to justify such expenditure. However, successful security operations at recent games raise questions about whether such expenditure is proportionate to the level of threat. The security budget is often cited as a reason why many cities will not host the Games. It has also been used by one city to justify their decision not to host the Winter Olympics even after it had been awarded. There are further problems. Not only must the organizers consider the security of the participants and visitors, they must also liaise with local and national security agencies to consider the potential threats against associated events and the supporting infrastructure.

Hence, the security demands can appear to be infinite. Traditionally, agencies have relied upon risk assessment techniques to address similar situations. Given that we cannot afford to meet all potential security threats, we must allocate finite resources to address those threats that are most likely or which pose the greatest consequences. However, the dynamic political and social context for many Games makes it difficult to validate the findings of any security risk assessment. There will, therefore, continue to be great uncertainty about the sufficiency of security measures for future Games.

2. *Accessibility versus protection.* The Olympics are by their nature one of the most difficult events to secure. They were revived with the specific intention of fostering peace between competing nations. Security measures are, therefore, often resented as a reminder of the problems that the modern movement was established to address. Security teams can also come into conflict with the expectations of athletes. Competitors have diverse training and personal requirements that create potential risks, which they would not face during normal competitions. The continuing need to confirm their identity and to carry documentation can be difficult for individuals who are preoccupied with their personal performance. The same comments apply to national officials and to coaches. It is possible to identify common 'flash points' where security conflicts with the participants' expectations. For example, recent games have seen repeated attempts by competitors to 'plug in' personal computers into the Games' intranet in order to gain external Internet access. Similarly, the need for repeated identification in order to gain access to some venues after prolonged journeys on congested motorways continues to create conflict between participants and security teams. The conflict between security and access also affect the general public. The organizers of the Turin games advised spectators to leave more than three hours to enter some venues for the 2006 winter games. Such warnings at least have the benefit that people can prepare for the delays. However, such delays raise important questions about how long it is reasonable to expect people to wait in order for security measures to be completed, especially when the sporting events themselves may only take a fraction of the time to enter the venue. These issues will not go away. Many sporting events now specify that entrance is tied to the person who is allocated the ticket. This creates delays and conflict when identification checks are conducted at the turn-styles.

3. *Technology versus timescales.* Previous sections have reviewed the technological, managerial and organization measures that have been taken to secure recent Olympics. However, the more elaborate these measures become then the more time that is needed to test the necessary infrastructure. Several recent Games have been struck by delays, in funding, in construction and in planning. These delays often seem to have minimal consequences to the high-level planning of the Games, which tends to focus on issues such as whether or not the Olympic stadium will be ready. However, it is easy to overlook the knock-on effect that these delays have on necessary testing of security measures. As a result, evacuation and marshalling drills may have to be conducted in venues that resemble the eventual location for Olympic events. This is far from ideal. For instance, three months before the Athens Olympics only 24 out the 39 Olympic venues were completed. Part of a 32km suburban rail connection to the Athens airport had not been started and a 24km tramway to carry spectators to the coastal venues was still under construction (BBC, 2004a). Such delays extend beyond the physical infrastructure and also affect information networks. The use of advanced software at the Athens Games provided new levels of access control over security information technology. However, the full, integrated system only came on-line weeks before the Games started. This created considerable challenges for the security team who had to plan for the use of critical information well before it became available over the data networks.

4. *Multi-agency, international approaches versus coordination overheads.* Recent games have seen increasing cooperation between security agencies both within and between countries. For example, the specialist staff recruited to organize the security at Olympic venues can be joined by officers from local police, from military and paramilitary forces. They can also draw upon support from immigration agencies concerned about illegal entry by competitors or visitors to the Games. Security teams may also have to draw upon specialist expertise from local agencies involved in nuclear, chemical and biological protection. They must liaise with healthcare agencies both to plan for emergency response and to coordinate more routine provision for spectators and competitors. At an international level, organizing committees have drawn upon help from NATO, INTERPOL, the FBI, the Israeli defense forces etc. In consequence, one of the first actions by Turin's TOROC organizing committee was to establish memorandums between their security group and the multiple agencies that they had to interact with. The concern was to ensure that critical issues were not overlooked at the interface between all of these different stakeholders.

5. *Low-profile versus Pre-emptive Policing.* Recent Games have posed particular problems for national security agencies in determining appropriate policies for the Olympics. For example, Australian police were widely criticized for a 'heavy handed' approach to demonstrators against the World Economic Forum in Melbourne. It can be argued that the use of riot police was intended to dissuade similar protests that might have disrupted the Sydney games. Similarly, the Italian police were criticized for their actions against environmental protestors who opposed the

development of a high-speed train link prior to the Turin Olympics. At another level, a series of raids against Islamic groups and the expulsion of individuals from Italy were clearly in preparation for the Winter Games. Such actions can be counter-productive if they provoke a violent response from disaffected groups. In the past, it has been possible for security forces to prevent clashes from marring the running of the Olympic events.

Previous sections have reviewed the assets that are vulnerable to attack during Olympic events. These include spectators, athletes, flagship events including the opening and closing ceremonies, media attention and the kudos of the Games, sponsors, vulnerable events such as the torch procession and the road races, the games infrastructure, the infrastructure of the host nation, co-located events such as the World Economic Forum, and security teams themselves. We have also reviewed a number of different threats, including malicious terrorist attacks from well funded groups through to similar attacks by disaffected individuals. We have also considered less extreme threats from groups of demonstrators and from individuals who use the Games to publicize political positions and commercial interests. Finally, we have argued that there are several important tensions that must be addressed by the security teams at future Olympic Games. Although the budgets are large, they are finite whereas the demands for security are almost infinite. This creates problems because it can be difficult to apply risk-based approaches to guide the allocation of security resources. Secondly, there are conflicts between the need to ensure security and the need to support the wider objectives of the athletes, coaches, spectators and organizers. Further problems arise from the time constraints that all recent games have operated under. Delays in construction and funding together with the perceived need to use the most advanced technology combine to limit the time that is available to verify and validate security measures. Similarly, the increasing need to coordinate diverse national and international agencies can increase communications overheads and may lead to break down in passing on key intelligence prior to the Games. Finally, organizers and security teams must identify an appropriate blend of pre-emptive measures and low-profile approaches to security. It may be better to act before disaffected groups can pose of coherent security threat. However, this can trigger other groups into action and may reveal important information sources that compromise other aspects of security.

5. Addressing Olympic Security Problems: Interactive Simulation Software

There are no panaceas for the problems that are summarised in the previous paragraph. Each organising committee and security team must address these constraints given the resources to hand and the available threat assessments. There are, however, a number of techniques that address some of the problems that complicate security planning for the Games. For example, biometric access control has been deployed to reduce the delays that athletes and organisers have faced when entering Olympic venues (Rosencrance, 2006). Conversational information retrieval systems have been developed to provide a common interface to the multiple intelligence databases being operated by independent security agencies both within and between countries. Tuple-space software enables analysts to issue requests for information that persist in the system for days, weeks or months (Johnson, 2004). Answers are then sent back to the analyst when and if the data that they seek is eventually entered into the system thus reducing the need for an individual to repeat their queries again and again in order to check for new information. Brevity prevents a complete review of the new organisational and technical developments that support security teams. In contrast, the remainder of this paper shows how computer-based evacuation simulations can be used to help prepare for the marshalling and policing of Olympic venues before those sites are built. This addresses the problems caused by construction delays that can severely limit opportunities for live drills and can prevent the results of those exercises from being used to alter the detailed layout of a venue before the competition takes place.

Security plans are typically, based around a relatively small number of scenarios. These often suffer from hindsight bias; organizations devote most resources to incidents that have occurred in the immediate past. It seems clear that recent games have been concerned to address any recurrence of the Munich and Atlanta attacks. Recent security teams have also deployed considerable resources to deter any use of commercial aircraft to attack Games venues. Security and emergency response plans can also suffer from a limited horizon; organizations do not consider the knock-on effects from an initial attack. For example, plans often focus on the immediate medical and security response without considering the crowd control issues that arise from those who are not immediately involved in an incident (Johnson, 2005). Similarly, it can be difficult to anticipate the consequences of any large-scale attacks on the digital infrastructure. Security plans are gradually refined over time using drills and exercises. However, these rehearsals further constrain the range of scenarios that are considered. They are expensive and can disrupt construction for the Games. There also pose risks to participants especially for mass exercises involving members of the public.

Simulation software is increasingly being used to supplement **but not replace** live drills (UK Atomic Energy Authority, 2002). Security teams can use these tools to explore a wider range of scenarios than is possible using conventional exercises. Many of these tools exploit relatively sophisticated techniques, some of which are derived from the games industries. For example, group behaviours can be modelled to simulate the 'flocking' that occurs when crowd move towards a common exit following a security incident. Simulation software has also been used to model communication failures between security teams (Johnson, 2005). Similarly, it is possible to simulate the interaction between multiple, simultaneous adverse events in different locations.

These techniques are important because planners can use simulations to alter the scenarios that are generated each time they interact with the system. Figure 2 provides an overview of the ways in which simulators can be integrated into more conventional forms of security planning. As can be seen, the approach begins by identifying the source of any potential threat. Previous sections have categorised these in terms of individual and group attacks along a continuum from the relatively 'benign' to more 'malicious' threats.

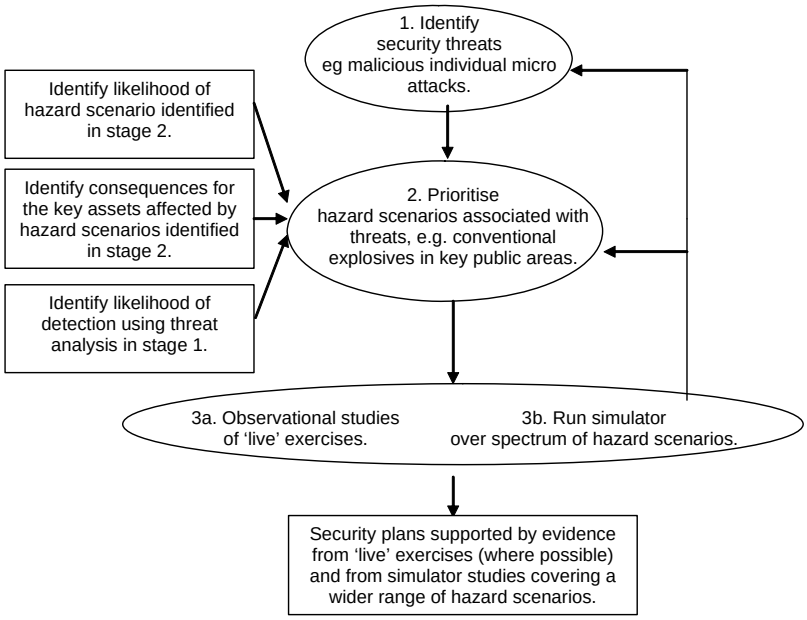

Figure 2: Integrating Simulator Software into Security Threat Assessment

The second stage focuses more narrowly on the hazard scenarios that are associated with these different threats. For example, nuclear and biochemical attacks are strongly associated with large scale, malicious attacks by organised groups. The use of improvised explosive devices characterise the actions of disaffected individuals. However, the London and Madrid bombings also illustrate the near simultaneous use of multiple improvised devices by groups. These scenarios must be prioritised using risk assessment techniques. As shown in Figure 1, this typically involves analyzing the assets that are threatened by a particular scenario. Additional resources must be devoted to analyzing mass attacks on the national infrastructures. Correspondingly, fewer resources may be devoted to media intrusion. Security risk assessment must also consider the relative likelihood of these different scenarios. The relatively low consequences associated with media intrusions must be balanced against the high likelihood, or near certainty, of such actions. Conversely, the extremely high consequences of an attack on the host city's water supply must be balanced against the relatively low previous incidence rate of such attacks in the past. Of course, these examples illustrate the difficulties of risk assessment for security scenarios. Even if a scenario has not occurred in the past then there are few guarantees that it will not happen in the future. Similarly, we cannot rely on future incidents always having the relatively benign consequences that they have had in the past. For instance, we cannot assume that nobody will be killed as a result of investigative journalists testing security preparations because this does not appear to have happened at previous Games. The final element of a security risk assessment focuses on the likelihood of detection. When ranking particular scenarios, it is important to consider whether or not particular threats are more likely than others to be detected before they can have an adverse effect on the key assets identified in previous sections. As mentioned, it can be particularly difficult to detect disaffected individuals. Intelligence operations can provide additional information that helps to detect group threats, especially from those that are likely to have malicious intent. However, the availability of such information varies between different groups and this information must be considered when planning for the allocation of finite resources.

The third stage illustrated in Figure 2 consists of physical drills and exercises together with the development of computer-based simulations. Previous sections have emphasised the need to incorporate both techniques because of the tight deadlines associated with the construction of many Olympic venues. The costs associated with mass security exercises also limit the number of scenarios that can be considered during the validation of security policies. In contrast, computer-based simulations can be used both to plan the response to potential incidents and to train different teams without needing access to the final venue. The results of these virtual exercises can also be used to inform the construction of sites where time and budgets allow. This joint approach is now a standard part of military training in many countries (Ross et al, 2004). The insights derived from

the simulations and live drills often reveal further threats and hazards that were not considered during previous stages of a security analysis. For example, the Greek authorities were able to make significant changes in their security preparations following exercises at their coastal venues. Both simulations and drills help to validate security risk assessments; independent experts can be recruited to observe these exercises and identify any omissions or oversights. This is critical given the difficulties of estimating the likelihood and consequences of any potential attack. Finally, the output of this iterative process is a series of plans that are backed up by extensive live exercises, where these are possible, and by a wide range of alternate scenarios generated using computer-based simulation. These software systems gradually move from being used in the validation of risk assessments through to playing a more prominent role in training, as security teams rehearse their response to different scenarios.

It is important to note, however, that a number of caveats have to be raised about the use of simulations in this manner. Firstly, although these techniques have been widely used in other security domains, they have not previous played a major part in planning for Olympic events. Secondly, there is a danger that simulations place unnecessary constraints on the scenarios that are considered. The benefits of this approach are lost if security teams become too focused on the threats that are easy to model using a particular software environment. In such circumstances, skills and plans will be developed in a virtual environment that will be of little benefit in the 'real world'. Finally, these tools are costly to develop and resources may be better used on physical security measures. There are ways of reducing such criticisms. As we shall see, low cost software is available, for example, to simulate the evacuation of crowds from sporting venues. These systems can simulate terrorist incidents directly from the architect's CAD/CAM models. Hence they can directly inform the development of the venues so that security issues are considered from an early stage in the organisation of the Games rather than as an afterthought in the brief interval between the end of construction and the lighting of the Olympic flame.

5.1 Scenario A: Evacuating the Spectators

There have been a number of previous attempts to develop computer-based simulations of evacuation behavior from large public buildings (UK Atomic Energy Authority, 2002). For instance, the Fire Research Service's (UK Building Research Establishment, 2004) CRISP tool associates individual behaviours with each person being modelled. These are described in terms of actions, which may be abandoned, and substituted by new ones in response to changes in their environment. Individuals can be sent to investigate a potential hazard, to warn others etc. before starting an evacuation. Similarly, the EXODUS system can dynamically insert individuals during a simulation (Owen, Galea and Lawrence, 1996). This enables users to quickly model a range of alternate scenarios involving crowds of different sizes. EXODUS also models the impact of warnings and information sources on group behaviour. We have developed the Glasgow Evacuation Simulator (GES) partly in response to the lessons that were learned following the evacuation of the World Trade Centre complex (Johnson, 2005a). This tool is unusual in that it enables users to simulate some of the effects that emergency personnel and security teams can have on crowd behaviour.

Evacuation software relies upon models of human behaviour to drive their simulations. For example, many people will first try to establish the credibility of an alarm before starting to move away from a potential hazard towards a place of safety (Bryan, 1982). Simulations can mimic these findings by introducing a fixed delay into each run. However, more elaborate models can also be developed to consider the perceived threat posed by the alarm, the degree of preoccupation with other activities, familiarity with evacuation procedures etc. It is also important to consider the social factors that influence evacuation times. 'Flocking' describes how people are often attracted into areas that are already crowded (Tong and Carter, 1985). This 'safety in numbers' behaviour can act as a catalyst to flight. Similarly, personality traits such as assertiveness have been shown to influence decision-making and behaviour under stress. For example, the Transport Canada Personality Profile 2 (TCPP2) identifies 13 characteristics that influence behaviour during evacuations. Projections based on the results of their experimental studies suggest that 20% of people are 'highly assertive' or 'goal directed'. These individuals can have evacuation times that are up to 25% faster than the 15-18% of people who are classified as being in less goal-oriented groups (Latman, 2004). Several recent simulators, therefore, enable users to dynamically alter the crowd composition both in terms of their physiology and also their psychological characteristics, including 'agression' or 'assertiveness'.

Age and physical limitations determine the speeds at which people can evacuate from an Olympic venue. However, these characteristics cannot be viewed in isolation; a panicking individual is more likely to travel at greater speed than a person who is calm. In our GES tool, each person is assigned an initial speed. The default is 1.4 ms^{-1}, although individuals may wish to override this value to reflect evidence from live exercises. Probability distributions are used so that the system will assign some individuals to be in either low or high-speed groups. These will move at 80% and 120% of the default value (Thompson and Marchant, 1995). These initial values are based on empirical observations that take into account individual pace under different crowd densities. The preferred walking speed of evacuation is sustained unless they cannot make any further progress because one or more people in front of them blocks their path.

The Glasgow Evacuation Simulator (GES) relies on Monte Carlo techniques to introduce non-deterministic behaviour into scenarios. This is important if security teams are to use the software in training exercises. The use of Monte Carlo techniques ensures that users can be faced with different incidents every time they run the simulator. Random numbers are generated and then compared against probability distributions to help simulate individual and group behaviours. This ensures that members of the public do not always follow the same course of action during each run of the simulation. They are, however, more likely to perform those actions that are considered to be most probable during an incident. The probability of particular behaviours can be directly informed by previous incidents, for example by reference to the FBI files on the Atlanta bombing or by the Italian documents on the TAV protests. The simulations can also be calibrated using live exercises. In consequence, it supports the iterative approach illustrated in Figure 2. As mentioned, an innovative feature of the GES is that it generates 3D models from architects' design tools. Unlike many other simulators, there is no need to build specialized computer simulations of each venue. This reduces costs and allows a tight integration between the simulator and the design of such structures. This is critical for Olympic security where plans often have to be developed some time before a venue is completed.

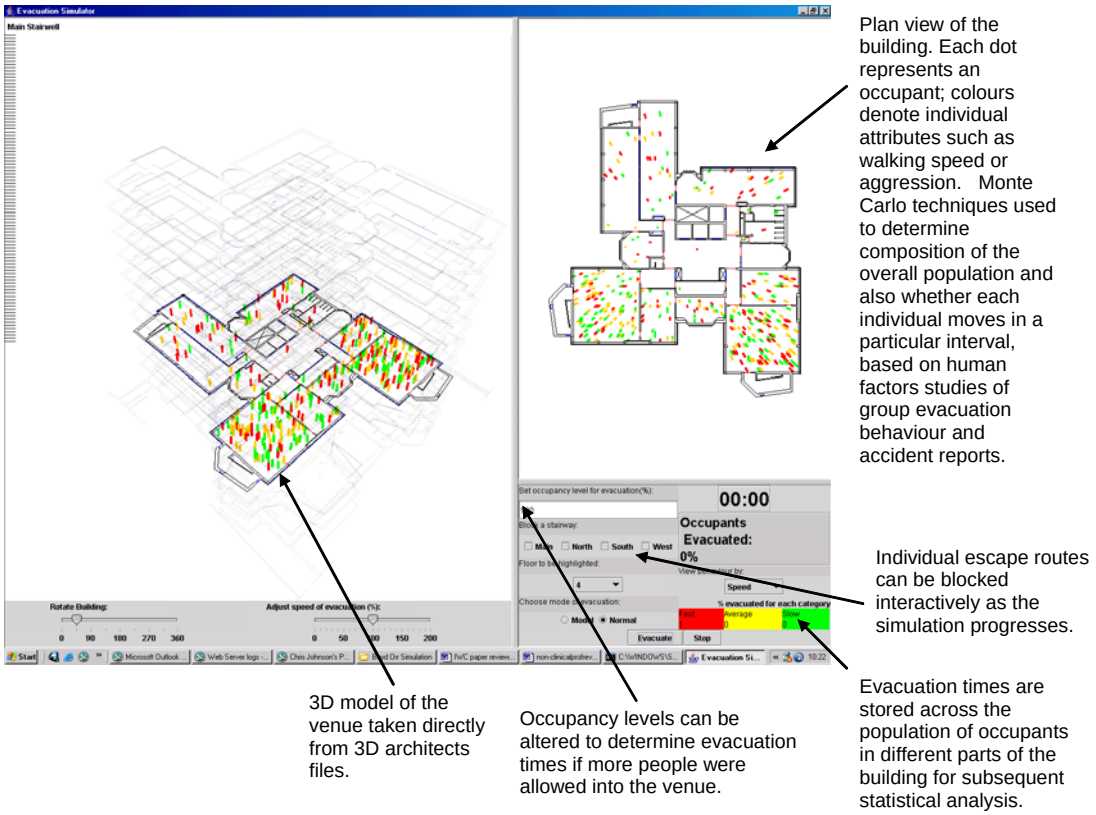

Figure 3: User Interface to the Glasgow Evacuation Simulator (GES)

Figure 3 illustrates the user interface to the GES software. As can be seen, users can vary the occupancy levels in a venue. They can also interactively open and close escape routes as a simulation progresses to model the effects of damage to the building or intervention from the emergency services. It is also possible to specify whether users will follow a 'model behaviour' in which they are likely to use the nearest available exit or a more expected behaviour in which most users retrace their steps back the way that they came into a venue. Figure 4 illustrates an application of the GES tool by analysing evacuation times when one of the escape routes is blocked. The top line shows mean evacuation times under different occupancy levels when occupants are likely to retrace their route into the building. The lower line provides the same information for 'model' evacuations in which each occupant attempts to exit by the nearest available route. The difference between the 'model' and 'normal' mean evacuation times is much greater than for any other emergency stairwells. Hence, considerable efforts should be made to ensure that occupants use this route in this venue rather than retracing their steps if they are to benefit from the time savings indicated in Figure 4.

The Glasgow Evacuation Simulator was specifically developed to model the behaviour of large groups of people. Initially, it was applied to help plan for the evacuation of large public buildings following the attacks of 11th September 2001. More recently, it has been used to review evacuation strategies for infrastructure projects including an urban underground train

system. It is currently being used to model the evacuation of a 50,000 seat soccer stadium. A common feature of these applications is the use of live exercises to calibrate the models. The intention is to maximise the number of scenarios that are considered whilst at the same time making the best use of limited drills. We have also used the insights from the simulations to change both procedures and the physical layout of these different venues. However, the focus has been on individual structures and much work remains to be done before we can be certain of the benefits that these tools might provide to an Olympic district on the scale of that proposed for the 2012 Games.

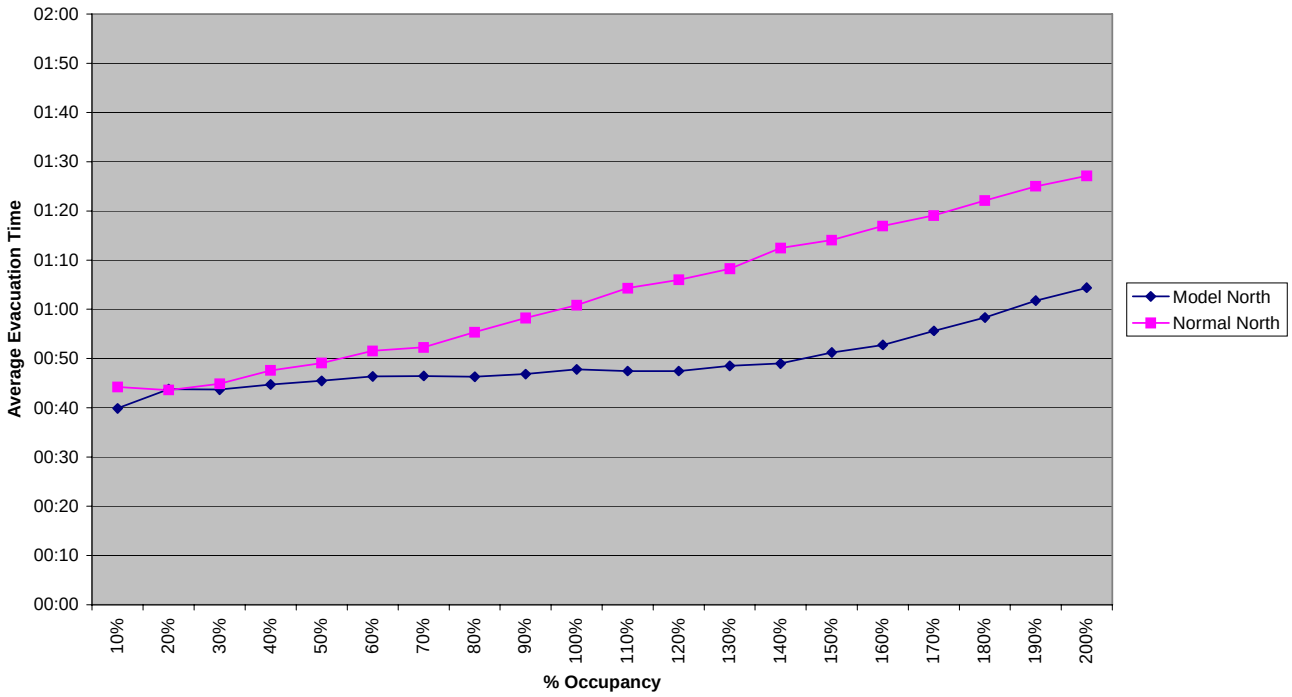

Figure 4: Graphing Mean Evacuation Times when an Escape Route is Closed

5.2 Scenario B: Modelling Security Teams

The simulation illustrated in Figure 3 shows how software tools can be used to model crowd behaviours in response to major security events. Monte Carlo techniques and used to control individual and group responses which are affected by the users interaction with the system, for example by directing the crowds towards particular exits or by introducing smoke into a venue. However, the previous analysis of Olympic security threats has also identified more focussed incidents, such as the Munich attacks, where far fewer people are involved. Simulators provide important tools that, if they are used creatively, can help to plan for such adverse events. For example, we have recently extended the GES tool to model the potential effects of a terrorist attack on a hospital complex. Most healthcare institutions use 'horizontal evacuation' techniques in response to a potential fire. Patients are not moved out of a building or onto another floor but are secured behind fire-resistant doors until help arrives from the emergency services. This policy will not provide adequate protection if a coordinated attack delayed the arrival of the fire services. This represents a significant vulnerability because our live drills and simulator studies show that for many UK hospitals it can take more than an hour to complete a partial horizontal evacuation, for example with night staffing levels and the presence of agency staff who are unfamiliar with the layout of particular wards. In order to make these predictions, it is necessary to simulate the way in which teams of trained staff will react to such security incidents. In the case of a terrorist attack on a hospital, nurses will typically respond by moving all patients in immediate danger. Next ambulatory patients and visitors are moved. Wheelchair patients are grouped together and then moved gradually to a place of safety. Finally, non-ambulatory patients are 'horizontally' evacuated. Those who can be transferred most easily are moved before those who require significant additional preparation. The implicit objective at each stage is to maximize the number of people who can be evacuated in the shortest available period of time.

Simulating the detailed plans of trained teams requires techniques that are very different from the stochastic behaviors of large crowds at sporting venues. Figure 5 illustrates the user interface to such a simulation. Readers who are concerned more with the application of these tools rather than the computational details should move on to the next paragraph. The implementation of the evacuation team is based around autonomous threads. The program creates an independent process for each individual. These processes can communicate through a form of message passing. The 'actions' performed by each nurse or security officer will change in response to the state of their environment. A form of reactive route finding is implemented using the A* algorithm that was first developed within the field of Artificial Intelligence. This assumes that each member of a security

team can identify each of the possible moves that they can make from their current location. They rank each of these moves and then only go on to consider the next set of available moves from the top ranked adjacent position. In this way, their planned route gradually grows as they always pick the best next step for further consideration. If a potential route becomes blocked then it may be necessary to consider the second route in the list of preferences. The success of the algorithm depends upon the choice of an appropriate heuristic. Euclidian distance can be used. Alternatively, more detailed information about the layout of a venue can also be used to guide an evacuation. Recall that an independent thread represents each person in this simulation. Each member of staff will also be employing his or her own independent navigation strategy. It is, therefore, possible that contention will occur if, for example, two nurses attempt to move two beds along the same narrow corridor. This is entirely to be expected and specialist negotiation algorithms must then be used to resolve the bottleneck that is also a feature of 'live' evacuation drills. It also introduces the conflicting behaviors that characterize real security incidents, as is apparent from the previous analysis of the response to the Munich attacks at Firstenfeldbruck air base.

Figure 5: Modelling the Response of Trained Teams (Hospitals)

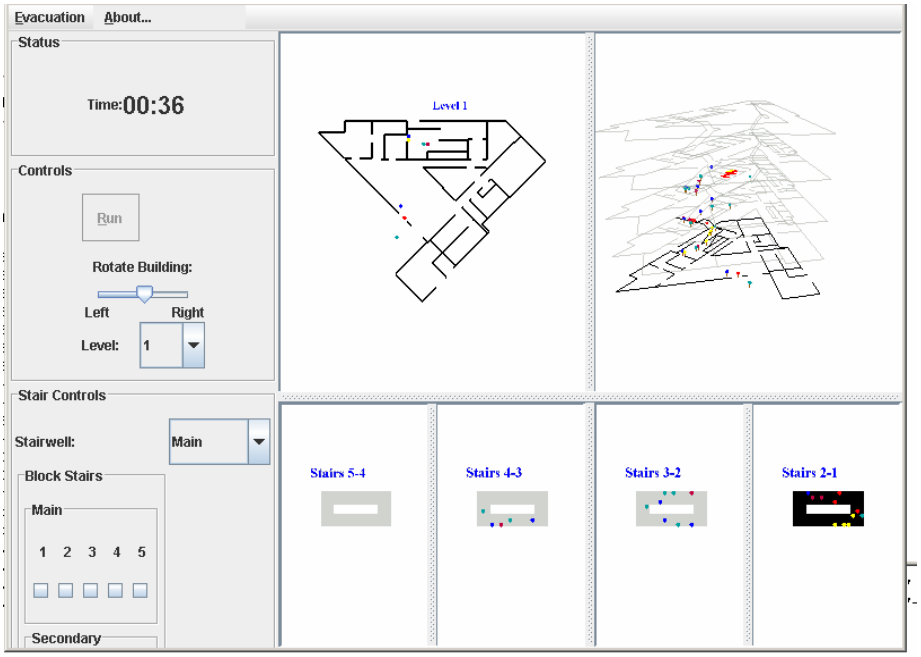

Figure 6: Modelling the Response of Trained Teams (Fire Crews)

Figure 6 represents the interface to another simulator. In this case, it is based on the architect's plans for a structure that is still being built as this paper is written. The top-right inset shows a number of individuals being evacuated through a three dimensional model of the proposed structure. The lower panes provide an overhead view of four stairwells. The lighter dots on 'Stairs 2-1' are emergency personnel trying to enter the building against the flow of occupants being evacuated. The loss of life amongst the Fire Department of New York personnel and the New York Police Department's Emergency Service Units in the World Trade Centre illustrates the importance of consider the deployment of external support in response to security incidents. As before, the software tool can be used to explore a range of different scenarios, including the number of occupants in the building, different numbers of emergency personnel being deployed in different teams, changes to the standard operating procedures for evacuating the building, alterations to the position and layout of the stairwells, the introduction of secondary incidents etc.

6. Conclusions

This paper began by reviewed the assets that are vulnerable to attack during Olympic events. These include spectators, athletes, sponsors, Games infrastructure, the infrastructure of the host nation and security teams themselves. Targets also included events that are critical for the kudos of the Olympics, including the opening and closing ceremonies. Previous attacks have also been aimed at particularly vulnerable events, such as the torch procession and the road races. Other targets are provided by co-located events, including the World Economic Forum that provided a focus for public protest before the Sydney summer Games in 2000. Later sections reviewed the different threats that might affect these assets. The analysis considered malicious attacks from well funded groups and disaffected individuals. It also considered threats from demonstrators and from individuals who use the Games to publicize political positions and commercial interests.

The analysis of the assets and threats facing security teams was based on a detailed survey of incidents at previous Games. These were then used to identify some of the constraints that affect security during the Olympics. Although the budgets are large, they are finite. The demands for security seem infinite. This creates problems because it is difficult to apply risk-based approaches to guide the allocation of security resources. Secondly, there are conflicts between the need to ensure security and the need to support the wider objectives of the athletes, coaches, spectators and organizers. Further problems arise from the time constraints that all recent games have operated under. Delays in construction and funding together with the perceived need to use the most advanced technology combine to limit the time that is available to verify and validate security measures. Similarly, the increasing need to coordinate diverse national and international agencies can increase communications overheads and may lead to break down in passing on key intelligence prior to the Games. Finally, organizers and security teams must identify an appropriate blend of pre-emptive measures and low-profile approaches to security. It may be better to act before disaffected groups can pose of coherent security threat. However, this can trigger other groups into action and may reveal important information sources that compromise other aspects of security.

The closing sections of this paper have presented one means of addressing some of these problems. It is critical that emergency response units and security teams avoid the problems that affected the Munich rescue attempt and the dispatching delays following the Atlanta bombing. However, we are unlikely to eliminate the delays and compromises that affect the construction of most Olympic venues. It is also difficult to manually consider a broad range of potential hazard scenarios either during the design of stadiums or in security planning. Computer simulation techniques can be used early in planning when there is some prospect of affecting the detailed layout of key sites. They can also be used closer to the Games, as training tools to rehearse key tactics and standard operating procedures before live drills can be conducted. However, a number of caveats must be raised. Although most of the existing techniques have been widely used within the United States military (Ross et al, 2004), they have not been used to support the security of Olympic events. These tools will only be successful if they can be successfully integrated into the working practices of the security teams for future Games.

Acknowledgements

This paper analyses a number of events that continue to provoke controversy and debate, especially the Munch attacks and the Atlanta pipe bombing. Every attempt has been made to provide a balanced account using publicly available sources. However, the intention is that the electronic version of this report will be updated and revised if the author is notified of any errors or omissions at the address given at the beginning of the paper.

References

Associated Press, Athens Security Budget Leaps 25 Percent, Thursday, 16th October, 2003.

Associated Press, Man Threatens To Attack Olympic Computers: Would-Be Hacker Under Investigation; No Charges Yet Filed, 13th February, 2006.

Associated Press, Security Tightened at Turin Olympics Venues. Filed by A. David, 30th January 2006a.

BBC Online, Australia Steps Up Olympic Security, 2000. Filed by Phil Mercer in Sydney.
Available on http://news.bbc.co.uk/1/hi/world/asia-pacific/924663.stm, last accessed 8th March 2006.

BBC Online, Q&A: Olympics security, 5th May 2004.
Available on http://news.bbc.co.uk/1/hi/world/europe/3686379.stm, last accessed 8th March 2006.

BBC Online, Viewpoint: Olympic mess of a preparation. Filed by G. Kassimeris, 26th March 2004a.
Available on http://news.bbc.co.uk/1/hi/world/europe/3568341.stm, last accessed 8th March 2006.

J.L. Bryan, Human behavior in the MGM Grand Hotel fire. Fire Journal. 76:37–48, March 1982.

Guardian, Divided We Fall. Filed by P. Barkham, 13th September 2000. Available on
http://www.guardian.co.uk/sydney/story/0,7369,367879,00.html, last accessed 8th March 2006.

C.W. Johnson, A Handbook of Accident and Incident Reporting, Glasgow University Press, Glasgow, United Kingdom, 2004.

C.W. Johnson, Applying the Lessons of the Attack on the World Trade Center, 11th September 2001, to the Design and Use of Interactive Evacuation Simulations, In Proceedings of ACM CHI 2005, ACM Press, New York, USA, 651-660, 2005.

C.W. Johnson, Lessons from the Evacuation of the World Trade Center, Sept 11th 2001 for the Future Development of Computer Simulations, Cognition, Technology and Work, (7)214-240, 2005a.

N. Latman, TCPP Personality Profile, In The Fourth Triennial International Fire and Cabin Safety Research Conference, 15-18 November 2004, Parque das Naçoes Conference Centre, Lisbon, Portugal, 2004.

NBC, Olympic Terror Concern Focuses On Two Fronts. Filed by R. Windrem, 8th February 2006. Available on http://www.msnbc.msn.com/id/11203844/page/2/, last accessed 8th March 2006.

M Owen, E Galea and P Lawrence, The EXODUS Evacuation Model Applied to Building Evacuation Scenarios. Journal of Fire Protection Engineering 1996, Vol.8(2), pp 65-86.

Reuters, Loner Seen As Main Olympics Security Threat, Filed by B. Goldsmith, Canberra, Australia, 30th August, 2000.

L. Rosencrance, Biometrics Used To Protect Germany's Olympic Athletes: Fingerprint Scanners From A Berlin Firm Limit Access To 'Deutsches Haus', Computerworld, 22nd February 2006.

K.G. Ross, G.A. Klein, P. Thunholm, J.F. Schmitt & H.C. Baxter, Recognition-Primed Decision Model, US Army Military Review, l:6-10, 2004.

San Fransico Chronicle, Police Outnumber Athletes 7-1 at Olympics: Safety is name of the Games. Filed by M. May, 12th August 2004.

P.A. Thompson and E.W. Marchant, Computer and fluid modelling of evacuation. *Safety Sci* **18**, pp. 277–289, 1995.

D. Tong and D. Canter, The Decision to Evacuate: A study of Motivations which Contribute to Evacuation in the Event of Fire. Fire Safety Journal 9:257-265. 1985.

TOROC (Turin Olympics Organising Committee), New Security Agreement With The Police For Defining Roles And Expertise, 1st December 2004.
Available on http://www.torino2006.org/ENG/OlympicGames/news/news_ita131989.html, last accessed 8th March 2006

UK Atomic Energy Authority, A Technical Summary of the AEA Egress Code, technical report AET/NOIL/27812001/002(2), Issue 1, Warrington UK, 2002.

UK Building Research Establishment, Evacuation Modeling: GridFlow and CRISP, Technical Report, Watford, UK, 2004.

Washington Post, Extraordinary Lengths Taken to Protect Olympics: Greece's $1.5 Billion Price Tag for Security Largest Ever for Games. Filed by A. Shipley and C. Whitlock, 12th August 2004.

White House, 2002. Preparing for the World: Homeland Security and Winter Olympics, Press release January 10, 2002, Available on http://www.whitehouse.gov/news/releases/2002/01/20020110-7.html, last accessed 8th March 2006.