

## **Security at the Olympics – far more than a stop and search process**

In the wake of the worst riots the UK has seen for decades, politicians, police and ordinary people are aghast that such mayhem could spread so violently, so quickly – and so simply.

From one incident, the UK's capital city was left burning, the flames licking out to other major cities in England. The aftermath brought the reality that social networking sites – Twitter, Facebook et al – were working overtime as gangs rallied troops from far and near to vent their so-called angst against the establishment. And then the BlackBerries went into overdrive as rioters spread the news that there was loot to be had and thousands converged on stores and shops to bag their free gifts.

This wasn't a 'bogof' situation it was a free for all as designer goods and electronics were passed through smashed doors and windows of some of the UK's leading retailers.

As the rubble is being sifted over, it's a time to reflect – not on what has happened, but what could have happened were the riots to have taken place this time next year. Imagine the total mayhem which would be caused had the rioting been slap bang in the middle of the Olympics 2012. Such would be the carnage that Britain could well implode.

The recent events were, essentially, rioting through cyberspace. Cyber space was used to rally deprived people to the cause and no one was able to stop it. Think of another scenario – we now know how rioting can be triggered by the press of a BlackBerry button: imagine that happening at the same time as a cyber attack is being made on the Olympics. Imagine a cyber attack which affects all the emergency lighting at the Games' venues; imagine too that a terrorist has been able to infiltrate the inner sanctums of security and, simultaneously, with the downing of the lighting, blows himself up...

Too scary to think about? Something out of a sci-fi movie? No... this is just something that could happen and last week's rioting has been a wake-up call for everyone to fret over. The word 'never' is now being replaced with 'could'.

The security surrounding such events as the Olympic Games is huge. And yet, despite that, incidents have happened during previous Games which have shocked the world. The worst by far was during the 1972 Munich Summer Olympics when members of Black September infiltrated the Olympic village, took members of the Israeli team and coaches hostage and then killed them.

/2

The main issue arising from that crisis was lack of effective security management. Since, security has been a prime consideration for the host countries of the Olympics. But incidents still occur and the 2012 Olympic Games is posing additional problems because of the technological advances which have been made since even the last Games in Beijing in 2008.

It was suggested in March this year that up to 1,000 extra public sector ICT jobs could be created in the run up to next year's Games. Indeed, according to a recruitment consultancy, an estimated 5,000 new ICT and telecoms jobs would be created as a whole as there is an unprecedented level of technology required for the 2012 event. This in turn presents cyber security problems.

Recently, Sir Malcolm Rifkind, former Defence Secretary and currently chairman of the Intelligence and Security Committee called for the UK to protect systems, educate people on threats and improve the ability to respond to state-sponsored cyber attacks. In an article, he wrote: "The last century saw armies engage on land, navies clash at sea, direct conflict in the air and cold war competition projected into space. In the new century, the threat of conflict has been extended into what some analysts now refer to as 'the fifth domain' – cyberspace.

When, just two decades ago, the internet was a system used mainly by academics and military researchers, today it is accessed by all and plays a huge part in our daily lives. In July this year, David Blunkett, former Home Secretary, admitted that the Labour government could have done more to tackle cyber crime – he was speaking at the launch of the International Cyber Security Protection Alliance (ICSPA) of which he is now chairman and, in an unprecedented show of support, he lauded the fact that the Coalition government was taking cyber threats seriously.

Since coming into government, the Coalition has announced the investment of some £63 million to tackle cyber crime – part of a wider £650 million cyber security investment. At a time when other budgets are being slashed, it's an indication of priority said Blunkett, adding: "The Coalition has elevated the whole issue of cyber – whether in terms of international threat or commercial and domestic threat - to a higher plane."

But is it too little, too late? There is a dire need for people to be trained from scratch to investigating cyber crime operations. Such training needs at least 18 months – and the Olympics are only 12 months away.

The public sector is also finding it difficult to recruit people and also to retain qualified professionals because the private sector, which pays more, is luring trained people away. But if next year's Olympics is to fulfil its IT needs, where will the people come from and, more importantly, will they be sufficiently and thoroughly security vetted?

/3

/3

Massimo Crottozzi a leading cyber crime expert who is MD of London-headquartered KCS Group's Information Services division said that he was originally concerned about security surrounding the Olympics on two counts – one being the hacking of the technology which is being installed and the other being the amount of specialist people needed to work it – and the credibility of these employees.

But he has since added his third concern – that social networking and BlackBerries could be infiltrated from afar to incite the riot-like situation which occurred last week. "It doesn't need a 'gang' as such to send out messages through Twitter etc, nor through the Blackberry and other such devices," said Crottozzi. "Remotely, someone can hack into systems, and there would be mayhem because we have already now seen that people – yes, even middle-class people who one would think would know better – have reacted in very irresponsible ways."

Crottozzi continued that there is urgent need to review in-depth the events of last week. "The police were left with little power over the sending of messages on the BBM (BlackBerry Messaging) system which brought more and more people into the fray. The police were caught out because, while BBM's maker, Research in Motion, can provide text content, they cannot provide the whereabouts of the mobile number – nor location – of the person(s) who sent out the inciting messages.

"There are systems available which can dig far more deeply and get to source, but it would be necessary for the authorities to incorporate access to such into their budgets – my advice is that this procedure should be a priority and finances should not be a consideration, to protect and safeguard, not just next year's Olympics, but everyday life of the decent citizen in the UK," Crottozzi said.

But while that is one issue which Crottozzi cites, his concerns range from hackers remotely infiltrating systems surrounding the Olympics' IT, to the people who are actively administering it. "On a simple level, and putting the word 'terrorism' aside at the moment, there is absolutely no question that the Olympics' IT system could be hacked into and data replicated to supply, for example, hundreds of counterfeit tickets. Equally, hackers could infiltrate to grab the personal details of everyone who subscribed to the site for tickets when it went on-line a few weeks ago. Their bank accounts are vulnerable."

Similarly, Crottozzi points out that the absolute screening processes necessary for the banks of IT professionals needed to successfully operate the Games is open to abuse. "Without being an alarmist there is the distinct possibility that an undesirable person who passes all the security tests for the job could be suspect and therefore cause a disaster from the inside. The authorities must tread carefully – seek very specialist advice - there's too much at stake."

#