Critical Essay

The London 2012 Olympic and Paralympic Games Olympic Intelligence Centre: Lessons Learned from Working with the Olympic Sponsors and the Private Sector

Sue Wilkinson

This paper is a reflective discussion that critically describes the role of the Olympic Intelligence Centre (OIC) played in the delivery of a safe and secure London 2012 Olympic and Paralympic Games. In particular, it examines how the OIC worked with the Olympic Sponsors and the wider private sector to provide them with the classified intelligence and information they needed to play their role in the safety and security operation effectively. Issues discussed include the cultural, statutory and systemic challenges that had to be overcome; how relationships were built to allay concerns and build trust and confidence; and the process that was put into place to allow the exchange of classified intelligence that supported the Sponsors and private sector in their operation. It details how the OIC worked with Sponsors to allow them in turn to exchange intelligence they held in their systems with the OIC, thus completing the intelligence cycle, enhancing the security operation. The article concludes with an outline of the lessons learned that were deduced through a reflective process and are offered to practitioners for consideration in future intelligence work involving the private sector.

Keywords: private intelligence; security intelligence; Olympic intelligence; terrorism; counterterrorism

BACKGROUND

The Olympic Intelligence Centre (OIC) was set up as a multi-agency "all-threats all-hazards" intelligence centre in support of the delivery of a safe and secure London 2012 Olympic and Paralympic Games (the Games). Its role was to be the single organization that protected the established UK intelligence infrastructure by providing a single point of contact for the Olympic-specific

intelligence operation, and managed and responded to demands and enquiries from what was a very wide and unique Olympic customer base. The OIC was at the centre of the threat assessment and intelligence gathering operation, and produced composite all-threat intelligence reports and problem profiling that no other organisation had the capacity, capability or appetite to deliver.

Over 100 organisations contributed intelligence, knowledge and assessment to the OIC. Potential threats included domestic and international terrorism, domestic extremism, protest and public order, serious and organized crime, international tensions and cyber threats as well as natural and malicious hazards. The OIC consolidated contributions into composite reports. Reports were produced across a range of classification levels, including, towards Games-time itself, at "non-protectively marked" (NPM)—such was the range of the demand. As well as regular all-threat intelligence reports, the OIC also produced threat assessments, briefings and responses to information requests from its wide range of customers—for example, on high profile individuals, crime groups, specific events such as the Olympic Torch Relay (OTR) and the Opening and Closing Ceremonies, and the likely impact of single issues on the Games, such as particular crime types or single threats.

All OIC products were designed for multiple use: by operational commanders to plan their mitigations and shape their operations; to provide the wider Olympic and Paralympic family with an accurate assessment of the threat picture; to inform security officials from some participating nations; to brief Government Departments and Ministers, national law enforcement agencies and the security and intelligence agencies, Olympic Sponsors and the wider private sector. Hence the need for reports at varying levels of classification.

"OLYMPIC INTELLIGENCE"—WORKING DEFINITION

The definition of "Olympic Intelligence" that the OIC worked to was agreed with all partners when the OIC was established:

> Intelligence that identifies or suggests a clear or direct threat to the security or safety of the London 2012 Olympic and Paralympic Games, including competitors, organisers, officials, venues and infrastructure;
>
> and/or

> Intelligence that identifies or suggests any criminality or action that either by its nature or association with the Games causes damage to the integrity of the Games.

It was clear that the private sector, and particularly the 55 Olympic Sponsors, would be affected by any number or combination of the identified threats. As the Games approached, it also became increasingly clear that the demand from them for a proper understanding of their own operating environment within the context of the Games would have a greater impact on the OIC and its contributors than had been originally anticipated.

THE OLYMPIC SPONSORS

There were 55 Olympic Sponsors altogether, providing a wide variety of support to Games delivery (These sponsors are listed in the Appendix). They ranged from large multi-nationals, to major British companies, to smaller enterprises, both British and foreign. They had varying expectations of the OIC, and some were far more interested in working closely and collaboratively than others. The OIC adapted its services accordingly.

Clearly, existing threats to some Olympic Sponsors could have implications for them and the Games, both in terms of general security and their corporate reputation. It was critically important to build a trusted relationship with Sponsors in order to be able to brief them in a secure environment, so that they in turn felt comfortable to share intelligence and information about their own vulnerabilities that would not normally be in the public domain, or even automatically shared with the police. Any inappropriate or inaccurate mishandling of private sector information or intelligence might have led to issues for commercial confidentiality, corporate reputation and brand name, and media issues which could, for example, even have affected share prices.

Many of the Olympic Sponsors (and other private sector partners) had excellent intelligence facilities of their own. There is no routine established, systematic and trusted common exchange of intelligence and information between the private sector and law enforcement in the UK, although many good and productive relationships and partnerships have always existed between different sets of partners for specific purposes.

With hindsight, the OIC was surprised at first when it became clear that many companies did not readily trust the OIC with their data and information,

and were very unwilling to share it, despite all the facilities and expertise the OIC had in place to ensure that their sensitive information was handled appropriately and confidentially. A great deal of collaborative work, planning and relationship building was needed to get to the point where the Sponsors were confident enough to entrust the OIC with appropriate intelligence.

From the OIC perspective, having access to the commercial intelligence and information on threats held by the Sponsors was essential to completing the all-threats intelligence picture. For example, companies were aware of their own protest issues, cyber vulnerabilities, serious and organized crime issues, insider threats—and had a good understanding of the impact of issues such as these on their operations. By extension, all of these threats might have security implications for the Games. Given how closely the safety and security program and the Sponsors had to work together on Games delivery, a mutual understanding of threats and intelligence relating to them was essential, to inform planning and decision making on keeping the Games safe—in terms of physical delivery, but also the integrity and reputation of all those involved (as per the definition of *Olympic Intelligence* above).

THE WIDER PRIVATE SECTOR

Staging an Olympic and Paralympic Games is an enterprise on an unprecedented scale. It involves massive engagement from across the private sector, large enterprises and small, just to keep multiple host cities and regions moving, serviced, supplied. Many of the issues described above in relation to Olympic Sponsors have a much wider application across national and local infrastructure. Sponsors were able to use their status to request Olympic-specific threat and intelligence briefings – but as the Games drew nearer it was clear that a range of other private sector providers across multiple sectors (utilities, transport, hotels, IT providers, the night-time economy as just a few examples) would not just want, but also need, informative briefings in order to operate and effectively fulfill their role in delivering a safe and secure Games.

THE OIC LIAISON TEAM

Formal engagement with Olympic Sponsors (and later the private sector) began in November 2011 after a dedicated Sponsors liaison officer was appointed to co-ordinate a small team. The OIC compiled profiles of all 55 Olympic Sponsors, and worked with other existing intelligence units, such as the National Domestic Extremism Unit, the Police Central e-Crime Unit, counter terrorism

units, and international liaison units, to assess the main threats to Sponsors. Successful ongoing engagement with the Sponsors, at regular briefings and also individual meetings, was critical to building their trust and confidence in the OIC, so that they in turn felt confident enough to share their own intelligence on threats—which in turn would lead to a more informed and effective security operation. Sponsors varied in their response but on the whole, OIC intelligence briefings were substantively enriched. The process of engagement continued right up to and throughout the Games thus ensuring that Sponsor profiles were kept up to date, and operational commanders were able to plan their safety and security mitigations accordingly.

THE KEY ISSUES AND DEBATES ON SHARING INTELLIGENCE WITH SPONSORS AND THE PRIVATE SECTOR

There was lengthy ongoing debate between the OIC and UK law enforcement, the security and intelligence agencies and with UK Government about what the nature and content of such briefings might be. At first the plan was that any briefings should be unclassified or "non-protectively marked." Given the UK's existing legislation, policy and practice in relation to classification and handling of such material, and the technical and intellectual question about whether there can be such a thing as an "unclassified" intelligence briefing, there was much discussion about whether the likely content of any such briefing was meaningful or of any practical use (The UK Government Protective Marking Scheme is included in the HMG Security Policy Framework and can be found at www.gov.uk). After much consideration by senior policy makers and practitioners, it was agreed such briefings could be compiled at RESTRICTED—subject to a suitably secure delivery method being devised.

Furthermore, some of the Sponsors (and some private sector partners) were international companies, which again affected what could be shared—some companies active in the Olympic sphere were from countries that did not have any form of established relationship or arrangements with the UK on sharing intelligence. The OIC had to be extremely careful of sharing information on Olympic threats and intelligence with foreign companies who might then, by default, be briefed on issues that their own governments were not. This was a political and diplomatic issue that again, was never fully resolved. The special nature of the Games allowed it to happen for the purposes of this event only.

The fact remains that the UK intelligence community does not widely share classified intelligence with the private sector on a routine basis. There are many systemic, structural and legal barriers to doing so. The challenge for the OIC was to develop trust and confidence enough, and to put in place a bespoke process to respond to the needs of this particular event. The reality of the statutory issues covering security, handling and accountability of both providers and recipients were met as far as they could be—training and awareness, handling restrictions and security clearances were put in place. Legal advice was sought but was not particularly conclusive. Had there been a leak or a security breach lessons would have been learned from the consequences—in the event, this was not tested.

Sponsors and private sector partners remained concerned throughout that any leaks or breaches might have a negative commercial or reputational impact on them. Their feedback to the OIC indicates that these fears were largely allayed by the processes that were put in place and the trusted relationships that were built up. The OIC, however, remained acutely aware throughout that private sector information and intelligence is commercially sensitive, and ensured it was treated with the same care and respect as any other crime or terrorism-related intelligence.

OIC intelligence reports could not be circulated by hand—a paper trail was assessed as too risky, even under established controlled handling conditions. Oral briefing of 55 Sponsors and others in a secure environment would have been logistically difficult to organize and time consuming, and briefing content would have been vulnerable to misinterpretation and onward cumulative inaccuracies. An IT solution put in place in partnership with the Centre for the Protection of National Infrastructure (CPNI) and described below, was assessed as the only viable option for sharing classified intelligence with Sponsors and the private sector (although paper circulation continued within established intelligence circles continued at RESTRICTED and at SECRET).

These arrangements were put into place incrementally, and regularly discussed at senior policy and program level throughout 2011 and into 2012, particularly as the program became more operational and entered the delivery phase from May 2012. The Olympic and Paralympic Games are such a global high profile and critically important event, a measure of pragmatism came into play—the very nature of the event allows for "special" arrangements to be made and agreed to meet the challenge. This is one of the huge opportunities offered

by hosting an event of this scale—to work differently, where doing so is the best way to meet the challenge.

THE OLYMPIC TORCH RELAY

The Olympic Torch Relay provides an excellent case study of law enforcement working closely with the private sector—in this case the three Olympic Sponsors of the Torch Relay, known as "The Presenting Partners"—Coca Cola (US), Samsung (South Korea) and LloydsTSB (now Lloyds Bank—UK).

For 70 days the Olympic Torch Relay crossed the UK, passing through high crime areas, inner cities, Northern Ireland and regions affected by a variety of local, national and international issues. Each of the Sponsors had pre-existing ongoing threats to them, particularly in the form of disruptive (as opposed to peaceful) protest. The Torch Relay was very high profile, and assessed as likely to attract attention from disruptive protestors, for example, whether protesting about their own causes and using the Torch Relay as a useful media backdrop, or protesting about the Sponsors, or against the staging of the Games. There were concerns about crime; and the period the Torch Relay passed through Northern Ireland was potentially challenging.

The Presenting Partners travelled ahead of the main body of the Relay in a convoy, engaging the crowds, handing out gifts, setting the scene. Clearly, they were potentially vulnerable, and had a strong argument for fuller intelligence briefings on a daily basis so they better understood the operating environment—to safeguard their own people, their convoy operation, and allow them to take account of upcoming issues such as expected protests in their own planning.

The business case for fuller briefing of the Presenting Partners was compelling, and it was agreed at senior policy level that given the unique circumstances of the Torch Relay RESTRICTED briefings would be made available to them. This broke new ground—intelligence was to be shared with international private sector partners, not in response to a single event or crisis where sharing intelligence might have been conducted as an exception, but on an ongoing basis as part of an extended operation. A process was put in place to provide a secure vehicle for physically getting the intelligence reports to the Presenting Partners.

THE INTELLIGENCE EXCHANGE IN PRACTICE

CPNI protects national security by providing protective security advice to public and private sector companies and organisations. Their advice covers physical security, personnel security and cyber security/information assurance on cyber and other threats, espionage and terrorism.

It was decided that CPNI would provide secure and bespoke access to OIC intelligence reports via its website, allowing accredited individuals to gain access to the reports through secure portals on the site. They would then be able to read a range of material, with access and content tailored to them and/or their organization, but they were not able to copy, alter, print or further disseminate the material—it was essentially provided on a "read-only" basis.

The CPNI solution was initially designed for the Presenting Partners on the Torch Relay; however, it was later decided to also invite all the Sponsors to apply to receive the briefings. All the Presenting Partners accepted, but not all Sponsors took up the offer. Those that did were asked to nominate an individual who would be the point of contact, and who would have to undergo a level of security clearance prior to being allowed access to the relevant secure portal. This might have been challenging to achieve, given the international organisations involved, but most companies locally employed security managers who were UK citizens so security checks were more straightforward to complete. Some Sponsors were in any case familiar with the CPNI website and used to working with it and with CPNI itself, so access approval was simpler. Nominated individuals initially completed an online security form and CPNI carried out further checks. They then attended OIC and CPNI briefings where they were provided with technical instructions and guidance for accessing the website, and an understanding of their role and responsibility in handling classified material.

Once nominated individuals had accessed the intelligence reports, it was their responsibility to forward brief on the contents within their own domain, to brief proportionately and appropriately, and take their own decisions on how best to achieve this. This was the assessed risk the OIC and CPNI took in achieving this outcome, and was covered in their induction process.

Once the decision had been taken to brief the Presenting Partners and then the Sponsors through CPNI, and it was clear that providers and recipients had confidence in the process, it was further agreed that some private sector

infrastructure providers who were already part of CPNI "business as usual" arrangements, would also have access to the OIC reports at CPNI's discretion. The same terms and conditions applied. By the time the Games were underway, the Presenting Partners, up to half the Sponsors, and a range of private sector organisations were in receipt of tailored classified (UK RESTRICTED) intelligence reports on Olympic threats. Customers of this service also had access as deemed appropriate to other reports such as event profiles—for example, the Opening and Closing ceremonies. At least some of the reports they were in receipt of contained intelligence and information they themselves had provided, thus completing a virtuous circle.

In addition, at Games time daily oral briefings for international security officials were hosted by the Olympic International Liaison Unit. An update on the day's events and likely issues were included on the agenda, and police commanders and other Olympic officials presented as needed—subjects covered might cover crime or likely protest, but also other issues such as transport, weather, or media. The police commanders used OIC RESTRICTED reports on which to base their briefings and were allowed to use their discretion on what was included and within what context—another example of fast-moving operational necessity over-riding normal precautions. It was decided that the Sponsors should also be invited to attend this briefing. OIC representatives were always present to take questions and deal with queries or concerns offline.

The OIC also produced unclassified briefings (non-protectively marked) that were forwarded to the Cross-sector Safety and Security Communications partnership, an initiative between the London Police Services, the Home Office, London First (a business networking organization) and 25 business sector groups. The partnership has created a communications structure via a telephone hub that enables members to be briefed on any relevant safety and security activity and how it might affect them. By the time briefings are disseminated many hundreds of people may have access to them, and the telephone hub is not secure. Therefore, briefings could only be unclassified. However, for the period of the Games, it was agreed that the OIC would produce a NPM briefing for inclusion at the daily telephone hub. This proved successful, but it is worth noting two things—first, that a meaningful briefing at NPM was far harder to achieve than was initially anticipated, and secondly, OIC staff were intelligence professionals and not accustomed to working in an unclassified environment, and extra training and familiarisation was required.

Feedback to the OIC and CPNI from the Sponsors and the private sector on this unprecedented range of engagement and briefing was, perhaps not surprisingly, overwhelmingly positive. The process allowed the private sector to better understand the environment within which the safety and security operation was being delivered, and allowed them to tailor their own operations and activities accordingly. With hindsight, the process should have been put in place earlier, and the intelligence cycle would then have been of a better quality earlier on in the planning phases in the years leading up to the Games. Nevertheless, there were also extensive lengthy discussions that took place at a senior governmental level, with the participating law enforcement and security and intelligence contributors, and with the Olympic delivery program, to achieve agreement to proceed—these arrangements were unique and innovative, and departed from normal practice.

LESSONS LEARNED

At the conclusion of the London 2012 Olympic and Paralympic Games in September 2012, an extensive de-brief process was undertaken on the entire intelligence operation, including with the Sponsors, and with partners of the OIC, as well as with the operational leadership group that ran the safety and security operation on a daily basis. Some clear principles emerged.

Because of the cross-sector, national and international nature of the Games, composite all-threat intelligence assessments and reports went to a far wider audience than is the norm under "business as usual." There were no security breaches that came to the attention of the OIC; no inappropriate sharing of information or intelligence was identified. All evidence indicated that the nominated individuals in receipt of the classified reports fully respected the terms and conditions and behaved entirely responsibly with the material made available to them.

The intelligence shared with the Sponsors and the private sector was at RESTRICTED only. That is not to say that had an emergency or critical incident occurred, one to one briefing at SECRET might have taken place as appropriate, as would also occur under "business as usual." But in order to achieve routine briefing at RESTRICTED, it was necessary for the contributing agencies and sources to provide their intelligence reports and assessments to the OIC at a lower classification than they normally operated at. In a fast moving, ongoing and dynamic environment such as the Olympics, SECRET reporting needs to be

at a minimum, as handling regulations then restrict access and circulation and, as operational commanders so often complain, intelligence in that format usually cannot be readily acted upon.

Therefore, the bulk of OIC material was made available at RESTRICTED—something that had not been originally anticipated. It became clear that in many cases an intelligence report at RESTRICTED did not necessarily differ hugely in content from the same report at SECRET. RESTRICTED intelligence reports could be more widely circulated, acted upon as necessary, and contained a version of the intelligence that might not have been circulated at all at SECRET. This posed the question of whether the UK intelligence community might routinely over-classify intelligence, thus inadvertently preventing wider circulation of safety and security information.

OIC intelligence reporting was routinely published in a composite all-threats format. All recipients, including the private sector, welcomed the ease of reference this provided. They also welcomed the fact that they could see threats together, allowing them to prioritise and assess the urgency of each in relation to another, thus assisting their decision making in terms of both response and allocation of resources. Normally, intelligence reports tend to be circulated by individual agencies on their area of reference only—for example, cyber, terrorism, serious and organized crime. By receiving all-threats reports they reported being able to read the reports more quickly, absorb the "whole picture" better, make prioritized decisions and manage their resources more effectively. If they wanted or needed greater detail this was provided on request to the OIC. Many of the Sponsors and private sector partners, unused to receiving intelligence reports at all, found the format and presentation of the reports user friendly from the start.

Composite all-threat intelligence reporting focused on an event the scale of the Games led, inevitably, to improved profiling - for example, of cyber threats and trends, protest profiling, links across the different threat areas that had not been identified in the same way before. It also highlighted intelligence gaps that the OIC addressed—for example, given the international nature of the Games, the OIC added the international protest picture to the national one to complete the analysis of likely disruptive activity in the UK over the summer of 2012. The contribution of the Sponsors and the wider private sector to the quality of composite all-threat reporting was significant, and endorses the value of the partnership with the Sponsors and the private sector that had been put in place.

CONCLUSION

There are many ongoing existing arrangements for engagement and information exchange with the private sector in the UK. CPNI have been cited in this paper. Police forces and law enforcement agencies routinely work closely with the private sector on prevention and detection of a wide variety of crime types—cyber, fraud, serious and organised crime, domestic extremism, terrorism to name but a few. In the event of critical incidents the normal classification rules can be lawfully put aside in the interests of an investigation and public safety. London First and the CSSC are but two examples of organisations that provide extensive networking opportunities and information exchange regularly, at an unclassified level.

The Games provided a unique opportunity to do things differently, to try out new ways of working within and across law enforcement, security and intelligence agencies, to test and adapt existing systems and processes. The integral role of the private sector in delivering a safe and secure Olympics demanded new arrangements. Over the recent past the private sector has increased its investment in intelligence, building impressive intelligence departments of their own, with a professionalised staff. The new arrangements developed to deliver the intelligence function in support of the Games delivered an enhanced intelligence picture for the benefit of all—as evidenced by the feedback from the private sector and law enforcement alike.

The *post*-Games challenge is to further test and assess the special arrangements that were put into place and extract critical learning and best practice, where appropriate building it in to "business as usual" systems and processes rather than allow it to remain particular to the Games period—and potentially forgotten.

DISCLAIMER

The critical commentary provided in this essay is by necessity nonspecific. This is because of the nature of the work it describes. As such, it has not been possible to cite specific examples of what was achieved. However, it is hoped the principles outlined here can be used when considering intelligence arrangements in the future—whether in support of a specific event, or for general application.

APPENDIX: LONDON 2012 OLYMPIC SPONSORS

1. Worldwide Partners—Coca-Cola; McDonalds; GE; Dow; Panasonic; Acer; Atos; Omega; Visa; P&G; and Samsung.
2. Official Partners: Tier One—Adidas; BMW; BP; British Airways; BT; EDF; LloydsTSB; and Procter & Gamble.
3. Official Partners: Tier Two—Adecco; ArcelorMittal; Cadbury; Cisco; Deloitte; Thomas Cook; and UPS.
4. Official Partners: Tier Three—Aggreko; Airwave; Atkins; The Boston Consulting Group; CBS Outdoor; Crystal CG; Eurostar; Freshfields Brickhaus Deringer LLP; G4S; GlaxoSmith-Kline; Gymnova; Heineken UK; Holiday Inn; John Lewis; McCann Worldgroup; Mondo; Nature Valley Granola Bars; Next; The Nielssen Company; Populous; Rapiscan Systems; Rio Tinto; Technogym; Thames Water; Ticketmaster; Trebor; Kathmandu Bazar Plaza; and Banjara Group

ABOUT THE AUTHOR

Sue Wilkinson holds a BA(Hons) degrees and was awarded the Queen's Police Medal. She joined the Metropolitan Police Service (MPS) in 1980, and held a variety of uniform, detective, policy, and strategy roles across London and at New Scotland Yard. She served in a variety of roles within the Specialist Crime Directorate before leaving for Australia in 2007 to take up a three year contract as the inaugural CEO of the Australia New Zealand Policing Advisory Agency (ANZPAA). When she returned to the Metropolitan Police Service in September 2010, Ms Wilkinson took on two roles—Head of Profession for Intelligence for the MPS, and Head of the Olympic Intelligence Centre and the National Olympic Intelligence Project for the London 2012 Olympic and Paralympics Games. In September 2011 Ms Wilkinson moved over to her Olympics role full-time. She has recently retired from the MPS following the success of the Olympics.

- o O o -