This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Setting the Agenda for an Evidence-based Olympics

Understanding the security agenda

RAND EUROPE

Contents

Summary 5

CHAPTER 1 **Understanding the risks** **7**
1.1 Terrorism at the Olympics 7
1.2 Targeted disruptions 8
1.3 Serious crime in connection with iconic events 8

CHAPTER 2 **Understanding the security agenda** **11**
2.1 The security environment in 2012 is unclear 11
2.2 An approach for developing potential future security environments 12
2.3 Defining potential security environments 15
2.4 Assessing the capability implications of potential environments 20
2.5 Thinking systematically about security in 2012 23

Summary

Big projects bring big challenges, and organising and running the Olympics is just about as big as it gets. Appropriate use of evidence can offer policymakers, organisers and implementers a way to create the right foundations for the decisions that will determine the success or failure of London's Olympic Games.

The full report on the evidence base for the London 2012 Olympics[1] covers three main aspects:

- A **meta-analysis** of policy areas that are pertinent to the planning, delivery and legacy of London 2012 using evidence from previous studies.

- A **research agenda for transport and infrastructure**, identified using modelling techniques that investigate the behaviour of travellers, the transport system and land use. The aim being to create systems that function effectively and efficiently during the Games and are sustainable systems post-Games.

- A method for **understanding the security agenda** for London 2012. Identifying a tool that can aid understanding of the interactions of different aspects of Olympic security - hostile intent; operational capability; and potential influences on security; thereby identify the security capabilities required to address different threats to security during London 2012.

Here we present the method for understanding the security risks faced by London 2012 and the security agenda that could be put in place to offset those risks.

RAND Europe is an independent not-for-profit research institute whose mission is to help improve policy and decision-making through research and analysis. RAND Europe's in-house teams offer multidisciplinary and multinational research strengths, both substantive and methodological. RAND Europe's work lies on the continuum between that of universities and consultancies, combining the academic rigour of universities and the professional, task oriented approach of consultancies. This study has been funded by RAND Corporation investment funding.

RAND Europe's Evidence Based Olympics Team is a cross-cutting research team drawing on expertise from all aspects of RAND Europe's public policy research. In the production

[1] RAND Europe (2007) 'Setting the agenda for an evidence based Olympics', TR-516, RAND Europe: Cambridge

of this report, the team would like to acknowledge the work of Lindsay Clutterbuck; Edward Nason; Ruth Levitt; Lisa Klautzer; Michael Hallsworth; Lila Rabinovich; Samir Puri; Greg Hannah; Aruna Sivakumar; Flavia Tsang; Peter Burge; and Cameron Munro. We would also like to acknowledge the contribution of Lynne Saylor; Kate Kirk; Jonathan Grant and Hans Pung for insightful comments on the report.

For more information about RAND Europe or this document, please email us at: Olympics@rand.org

CHAPTER 1 Understanding the risks

Olympic security must consider all aspects of the actual and potential threats. If such an integrated and holistic approach is not employed, organisers may fail to perceive how the Games are vulnerable to events that fall outside the parameters of conventional security thinking.

The security threat is diverse and wide-ranging. It encompasses a time-scale that is far greater than the period of the Games themselves and a geographical span that is far broader than the Olympic sites and venues. Similarly, the threat may originate from multiple sources with varying levels of organisation, from loosely connected associations to tightly coordinated teams. In essence, the security threat arises from three main areas: terrorism, targeted disruption and serious crime. These categories are not clearly delineated and there can be overlaps between them.

1.1 Terrorism at the Olympics

The Olympic Games have been subject to terrorist attacks on two occasions. The first was in Munich, West Germany, between September 5th and 6th, 1972, when the Israeli team were attacked in the Olympic Village by a terrorist group called Black September. This resulted in the death of eleven Israeli athletes and coaches, and all of the terrorists. The second took place in Atlanta, USA on July 27th, 1996. A pipe-bomb concealed in a rucksack was planted in the Centennial Olympic Park in Atlanta, Georgia, an area in continuous use as a venue for live music acts. In this attack, one person was killed and 100 were injured. No claim of responsibility was made. Terrorist attacks have been carried out during other major sporting events, such as the IRA attack in Manchester during the EURO 96 Football Championship.

These events illustrate the wide spectrum covered by the fields of terrorist organisation, motivation, objectives, targeting and tactics. It is therefore critical that the security arrangements for the London Games are comprehensive and flexible enough to reduce the overall risk from terrorism, as well as from specific threats that were mere possibilities in 1996 (and not conceived of at all in 1972). These may include attacks using chemical, biological, radiological and nuclear weapons (CBRN), or suicide terrorism. It is also important to look more widely than just at terrorism aimed directly at the Olympic Games.

From July 2003 onwards, a series of explosions occurred in Athens aimed at a variety of targets. The majority were claimed by 'Revolutionary Struggle', an extreme left-wing

terrorist group that continues to operate today. These attacks sowed doubt concerning the ability of the Greek police to protect the Games successfully. They also enabled Revolutionary Struggle to call a unilateral 'cease-fire' for the duration of the Games, thus enhancing the illusion of their power and influence. Terrorist attacks from whatever source that occur anywhere in the host city at any time prior to the Games generate a negative perception of the safety of the Games themselves. With the crucial role of sponsorship and the need for the organisers of any Olympics to maximise the return on investment, the implications of such attacks are clear.

1.2 Targeted disruptions

The G8 summit in Gleneagles, Scotland, during July 2005, provided the biggest test to date for the type of policing required to deal with a high-profile, combined security and potential public disorder threat. The simultaneous suicide bomb attacks in London on July 7th, the day after the 2012 Olympic Games had been awarded to London, shows that security planning must have a national and not just a local focus.

Until recently, public protest during an Olympic Games and its associated events was almost unheard of. The first inkling that this might change came in 2000, as protesters realised the potential of the Salt Lake City Games to raise their media profile. Protestors against animal cruelty used the opportunity of the passage of the Olympic torch to demonstrate against the holding of an 'Olympic Rodeo'.

This trend continued in advance of the Winter Games in Italy during 2006. The passage of the torch was dogged by anti-globalisation protestors (aimed at the main sponsor of the Games, Coca Cola), those who objected to what they saw as the increasing commercialisation of the Games, and local demonstrators who had no issue with the Games but saw it as an opportunity to protest against the advent of a forthcoming high-speed train link.

1.3 Serious crime in connection with iconic events

It appears that certain types of criminal develop the perception that, as police attention must be wholly focused on the mega event, there is an unrivalled opportunity for them to engage in a 'criminal spectacular' elsewhere. The opening day of the 1994 Lillehammer Winter Olympics provides an example. On that day, Edvard Munch's famous *Scream* painting was stolen from the Norwegian National Gallery in Oslo.

Other big events have also been used as cover for major thefts of art. St Patrick's Day is a widely-celebrated and significant social event in Boston, Massachusetts. On that day in 1990, several Rembrandts, a Vermeer and other significant works of art were stolen from the Isabella Stewart Gardner Museum. Closer to home but again embodying the same principles of distraction, Millenium Eve night in 1999/2000 saw the theft from the Ashmolean Museum, Oxford, of their only painting by Cezanne. The motivation behind all three of these examples was personal criminal gain.

In terms of identifying evidence on the security threats to the Olympics, there is a lot of evidence on strategies that did not work (or to put it another way, high profile security breaches). However, since the essence of security is to reduce threats, when it is successful it is rarely publicised and even more rarely evaluated. A more in-depth evaluation of the previous security regimes would require access to primary data sources as well as secondary ones, but it would undoubtedly allow a range of difficult questions to be addressed. The sorts of security threats that are likely to be in place during 2012 are very difficult to predict, however we suggest a futures matrix methodology to identify likely threats and security solutions for London 2012 in an attempt to provide evidence based security planning for the Games.

CHAPTER 2 Understanding the security agenda

"What is … certain is that the Games will focus the entire world's attention on London and the UK. More countries will participate at the London games in 2012 than there are members of the UN."[2]

Tony Blair, Former Prime Minister of the UK

2.1 The security environment in 2012 is unclear

Being at the centre of the world's attention as the host nation for the 2012 Olympic Games carries with it darker implications for London and the UK. In terms of security, there are immediate implications that go far beyond any future increased threat from terrorism in the UK and against UK interests world-wide during the period of the Games themselves. Along with China, the UK is one of only two countries in the world that have been chosen to host forthcoming Olympic Games. After the Beijing Games, the global perception of London and the UK will ratchet up further as the UK becomes the host nation for the *next* Olympics. Throughout this period, groups and individuals anxious to seek publicity and recognition for their myriad causes will have a window of opportunity to target London and the UK, knowing full well that they are guaranteed the level of global media coverage accorded to the designated host city and host nation.

Olympic sites and venues appear at first sight to be the most obvious targets for disruption and attack. However, the potential threat from terrorism and politically motivated crime must be seen in a wider context than the Games themselves. In terms of geography, the threat is likely to be not only to London but also to the UK nationally and to UK interests globally. In terms of time, threats already exist today and they are likely to become increasingly tangible between now and the start of the Games. Nor can it be assumed that the current range of threats will not broaden or intensify. As the security environment in 2012 is unclear, security requirements for the 2012 Games must be developed in the face of uncertainty.

[2] 'The Greenest Games Ever,' Tony Blair, *The Guardian*, 23 January 2007, p.26

While it is not possible to predict the security threats that may impact on the Games in five years time, it is possible to foresee the potential range of their scope and diversity. The meta analysis in Chapter 2 of the full report[3] highlights a number of instances in the past where large-scale sporting events, including the Olympic Games, have been exploited, targeted, disrupted or attacked to further specific causes, grievances or criminal enterprises. Based on this evidence, there is a clear need for operational and contingency planning to identify and counter a spectrum of threats to the 2012 Olympic Games, to London and to the UK. How is it possible to develop systematic and meaningful planning assumptions today that are relevant and appropriate to an event and time period that lies five years in the future?

2.2 An approach for developing potential future security environments

Trying to *predict* the future security environment five years in advance is a futile exercise. However, it is possible to try to *foresee* in a structured and systematic way a range of different potential security environments that could potentially exist in 2012. The purpose of doing this is to help understand the different implications these have for existing and future security capabilities.

RAND Europe has developed a model that separates the characteristics of any given future security environment (FSE) into three dimensions which are flexible and can be altered. The model does not give any specific weight to a particular future scenario, rather, it treats all futures as equally valid. The three dimensions have been chosen on the basis that it is reasonable to expect that threats to UK security will comprise an unpredictable combination of:

- **Adversary hostile intent:** This dimension focuses on the potential intent of any given terrorist or other actor that engages in security-threatening activities to further its objectives. These activities might range from the use of demonstrations, through sabotage, public disorder and mass casualty attacks. This dimension conveys the intent of a potential adversary through the scale of its ambitions, and by demonstrating the kinds of activities it could conduct.
- **Adversary operational capability:** This dimension focuses on the potential capabilities of the terrorist or other actor to utilise a range of violent and non-violent activities to further its objectives. The technical capabilities will vary from group to group and from individual to individual. While groups may intend to conduct significant activities, they may be constrained (or enhanced) by their level of technical competence. This dimension conveys the range of activities that may be undertaken.
- **Potential domestic/international influences on UK security:** This dimension focuses on the extent to which the overall UK and global situation in 2012 will act as a motivating force for terrorists or other actors. The goal is not to predict specific issues that will motivate future attackers. Rather, this dimension conveys

[3] RAND Europe (2007). Op Cit

the overall severity of the threat environment and the potential scale and tempo of threats it is likely to inspire. The baseline environment is taken as 2007. A worsening environment from 2007 is likely to mean a greater number of causes motivating potential attackers. An improving environment will not eliminate all threats, but will likely dampen their incidence and the order of magnitude.

Having established three defining dimensions, it is possible to combine them in order to imagine a number of future security environments. Each potential future security environment will be determined by the relationship between each of the three dimensions. We have chosen to represent this visually in a three-dimensional cube (Figure 1). If the near lower left-hand corner is assumed to be the origin of the cube, then that point will represent where each of our three dimensions are the most benign. As each dimensional axis moves right, up or back (respectively), the dimensions are assumed to become more intense, so that the greatest threat security-wise is in the upper back-right of the cube.

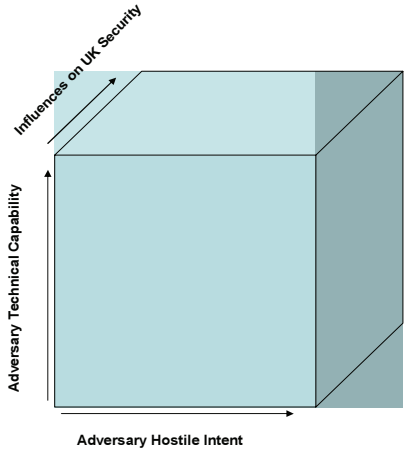

Figure 1. Representation of the three strands of security threat

To understand in more detail the progression along the each dimension from a more benign to a more severe position, three broad divisions have been drawn along each dimension (Figure 2).

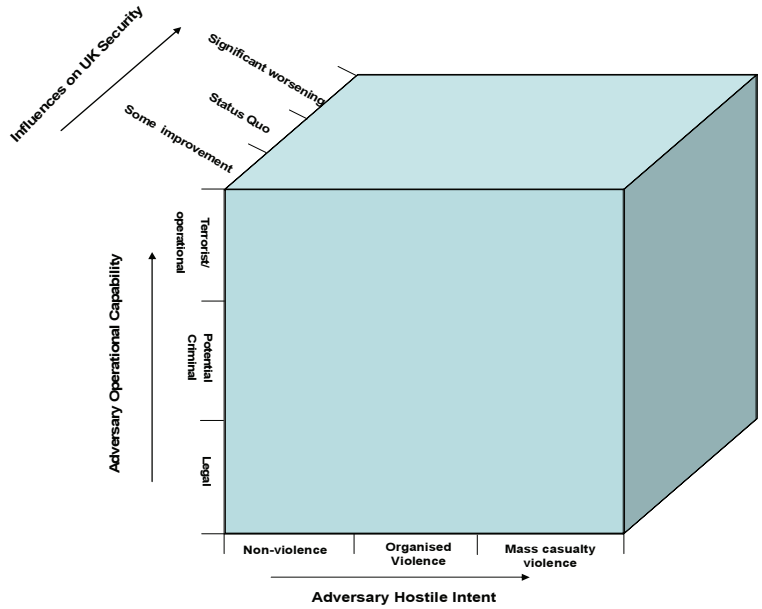

Figure 2. Dividing the security threat by risk

Having created a three-dimensional space that is able to illustrate a range of possible future threats, it is possible to segment that space into sub-cubes. By looking at how far along the dimensions each sub-cube is placed, we can characterise more precisely the security environment given this particular combination of adversary intent, capability and global situation. This produces 27 distinct sub-cubes, each representing a potential future security environment (Figure 3).

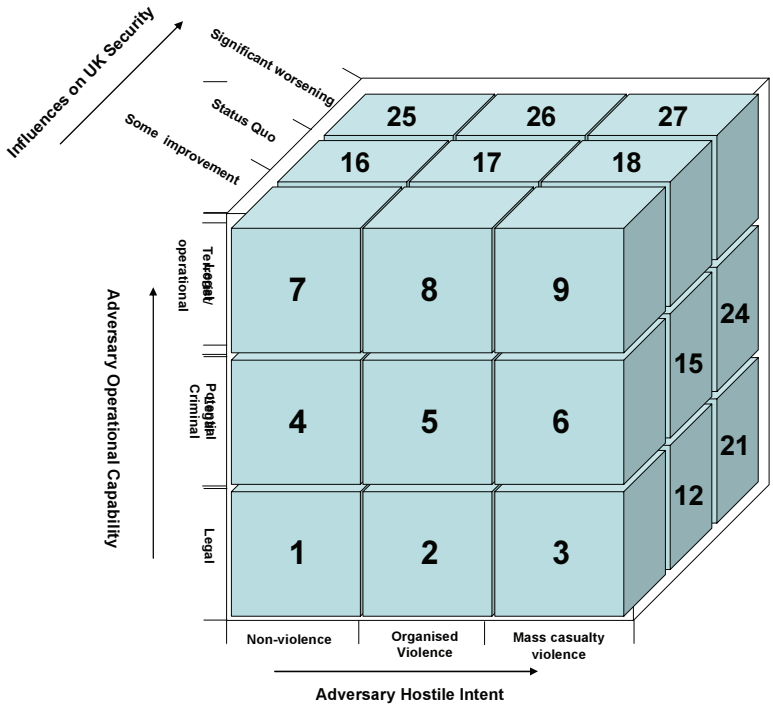

Figure 3. Dividing the future security environments

It is thus possible to visualise future threats to UK security as falling somewhere within a three-dimensional range of possibilities, from the most benign to the most insecure. The model helps to visualise how changing conditions will result in a changing position within the cube. As we near 2012, it will be increasingly possible to understand which future environments are more likely and which are less likely. This will bestow a degree of structure within which contingency planning can be carried out and those planning assumptions exercised.

The model treats each potential future security environment as equally valid. However, six of the sub-cubes produce an improbable combination of conditions. These are sub cubes 2, 3, 11, 12, 20 and 21, because organised violence or mass-casualty violence cannot be carried out legally. These cubes will be excluded from analysis.

2.3 Defining potential security environments

To illustrate how a range of scenarios can be constructed using the cube model, we have picked six sub-cubes that represent highly contrasting future environments. From this we can derive specific scenarios and understand their capability implications. The purpose of doing this is to display the range of possible threats that could exist, *not* to predict specific threats. Section 4.4 will examine the implications this range of scenarios has on the security apparatus that is required to meet these challenges. Not all of these illustrative scenarios relate directly the Olympic Games, reflecting the possibility that, while a direct assault on the Games is a possibility, security threats might arise with nothing more than tangential connections to the Olympics. Moreover, although many of these scenarios are London-centric, it must also be recognised that incidents may occur elsewhere in the UK as Games events are taking place in a number of locations – such incidents may be displacement attacks (i.e. not undertaken in London due to high levels of security there).[4] The following scenarios have been developed for illustrative purposes, and to facilitate the capability analysis in section 4.4.

Scenario 1: this is the most benign future security environment, in which groups challenging security around 2012 to further their objectives will do so using ostensibly legal, non-violent means in a global environment that represents some improvement from the level of instability in 2007. This corresponds to cube 1 (Figure 4).

[4] For example, the suicide bomb attacks that took place in London on July 7th 2005 occurred during the G8 summit that was in progress at Gleneagles in Scotland. The timing may have been coincidental but it illustrates the concept.

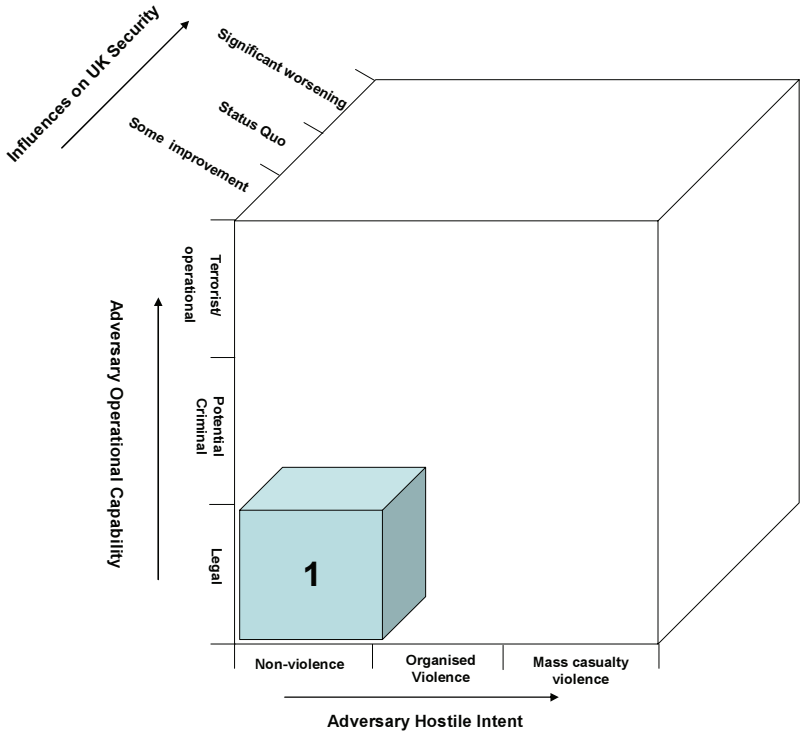

Figure 4. Future security scenario 1

Our illustrative scenario is of a single-issue protest group using the opportunity of the 2012 Olympics to highlight their cause. The group campaigns on a specific environmental issue, and stages a day of protests and peaceful blockades at numerous relevant locations such as petrol stations and major road intersections. The issue has lost some traction amongst the wider population. The core protesters compensate for their lack of mass human resources by operating on a swarming basis, dividing into a dozen different groups, each blocking a single site for a relatively short period of time during rush hour, before shifting location within central London. They coordinate movements using the latest mobile phone navigation technology, moving frequently enough to avoid all being swept up in one go.[5] This presents a public order challenge, although within a manageable scale.

Scenario 2: this is the future security environment that most closely resembles today. Some groups exist that seek to use terrorism to further their cause, while others posses the capability to cause public disorder. All of this takes place in an unstable global environment in which numerous issues exist that can inflame opinion and motivate attacks. It is represented by cube 14 (Figure 5).

[5] Historical precedents for this technique were the series of anarchic but pre-planned events that protestors staged during the 'J18' and 'N30' demonstrations of 1999 in London and again in London, the May Day protests over several years from the late 1990s onward.

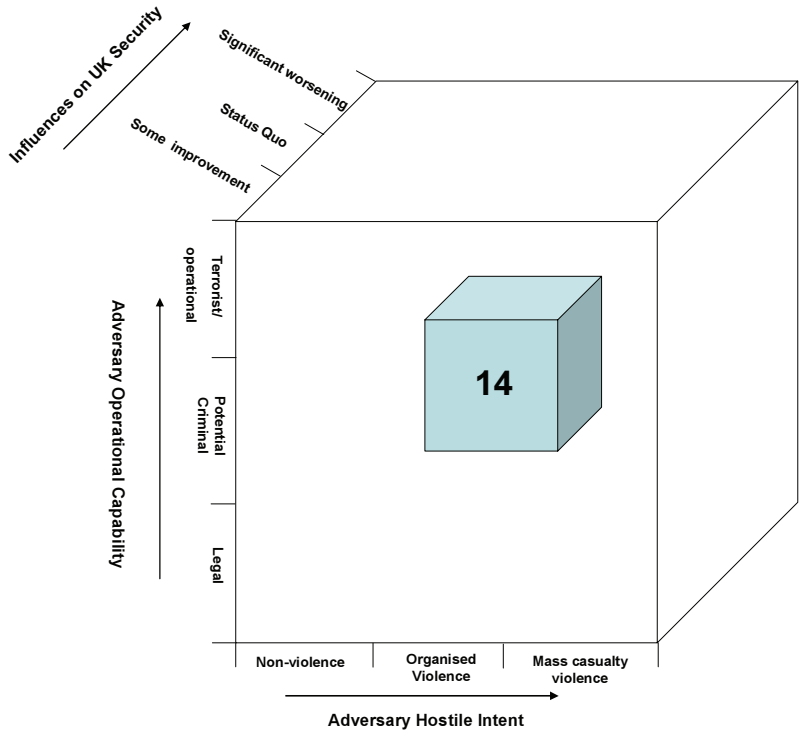

Figure 5. Future security scenario 2

Our illustrative scenario involves a radical element within a UK diaspora community that is planning to launch targeted violent strikes against international targets in London, hoping that the added global attention of the Olympics will serve to advance their cause.[6] They are motivated to undertake these attacks due to a worsening situation many miles away from the UK, as foreign armed forces clamp down on a nascent state arising out of the consequence of instability in the Middle East. Planned attacks include the kidnap or assassination of a foreign VIP, and a bomb attack against a foreign embassy. The attackers are at the preparatory stage, having formed the intent for an attack and assembled enough personnel to mount it. They are now located in a safe house and are well advanced in acquiring the necessary materials.

Scenario 3: this is the most unstable future security environment, in which multiple groups exist possessing the intent and the appropriate operational capabilities to mount mass-casualty attacks. The global environment has worsened to the degree that multiple causes exist to aggrieve and motivate attackers, increasing both the potential severity of attacks, and the potential frequency of their occurrence. It is represented in cube 27 (Figure 6).

[6] The hostage crisis at the Olympics in Munich in 1972 serves as a broad historical precedent.

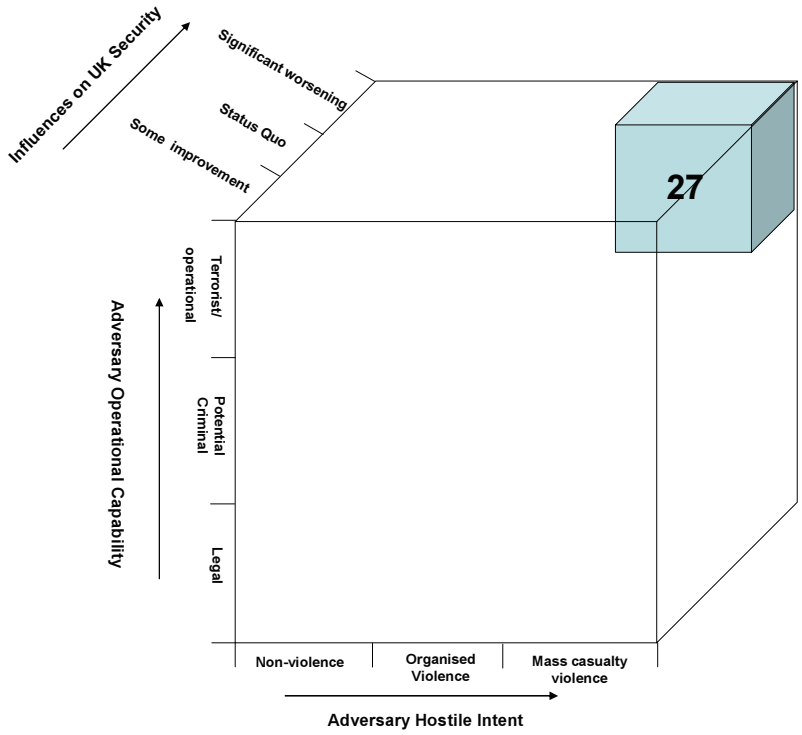

Figure 6. Future security scenario 3

Our illustrative scenario revolves around several simultaneous bomb attacks. Race relations in the UK have degraded significantly from today, and different communities have become highly polarized and insular. Domestic white supremacist groups have decided to defy the international goodwill message of the Olympics by mounting a series of mass-casualty attacks against a particular UK migrant community.[7] They have carried out a coordinated series of vehicle-borne remote-detonated explosions against several important religious sites in London, causing significant casualties. This has been followed by a propaganda campaign on the internet including threats of further attacks unless the Government reverses its policy on immigration and multiculturalism. The security implications are considerable; the degradation in UK social cohesion will decrease the amount and quality of intelligence and information received by the authorities regarding terrorist activities. The emphasis will move to post-attack management, and managing the information fallout will demand strong public diplomacy to stem outrage and to prevent mass public disorder.

Scenario 4: this scenario represents a similar degree of global instability to today, but one that is populated by groups possessing both the intent and the sophistication to mount devastating mass-casualty attacks. It is represented by cube 17 (Figure 7).

[7] The immediate detrimental effect of specific communities that perceive themselves to be directly under attack has been seen before in events as diverse as the nail-bomb attacks carried out by David Copeland in Brixton and Brick Lane during April 1999 and the severe public disorder in Lewisham (1977) and Southall (1979) following events organised by outside extreme-right wing elements and seen as provocative by the local community.

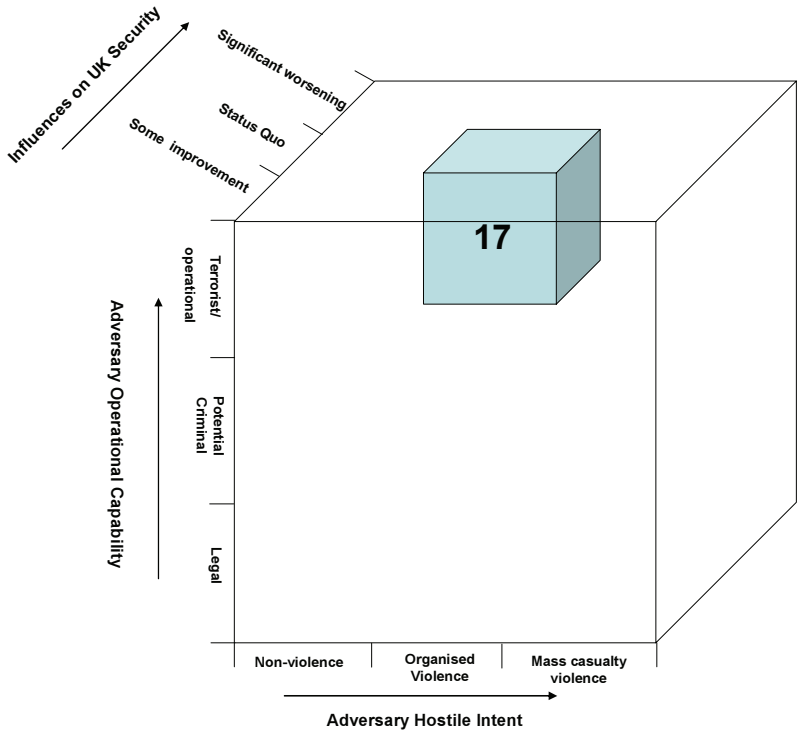

Figure 7. Future security scenario 4

This illustrative scenario concerns an attack mounted by a Jihadist cell aligned with al-Qaida's ideological worldview. Seeking to inflict significant casualties during the Games, the cell has mounted a number of effective attacks, occurring near-simultaneously. These attacks consisted of the use of suicide bombs, detonated during a morning in the lobby of four leading central hotels, with the apparent aim of targeting representatives of several Western Olympic teams. These four attacks caused significant loss of life and damage to the hotels, with subsequent disruption to the surrounding areas.

Scenario 5: this scenario takes place in the same future as scenario 4 and is therefore also represented by cube 17 (illustrated in Figure 7). It is provided as an illustrative example of how a different attacker modus operandi will demand different a security response, albeit within the same future environment.

In this scenario, an individual has taken a container of an unknown chemical liquid aboard a busy London Underground train during rush hour. Immediately prior to its departure from a major London station, the individual opens the container and allows the chemical to spill onto the floor of the carriage, he then leaves the train as the doors are closing. As the train moves to the next station, a large number of passengers aboard the carriage are overcome by the chemical, with symptoms including vomiting and respiratory difficulties. With the passenger emergency alarm having been activated, the train goes to the next station, stops, and its doors open. Those passengers not incapacitated attempt to flee the train, intermingling with passengers already on the platform and seeking to escape from the Underground network via the station's exits.

Scenario 6: this scenario takes place in a global environment that exhibits some improvement from today. However, it is recognised that hardcore support for, or resistance

against, certain issues may persist even in the absence of wider traction among the public. The groups discussed in this scenario are in the planning stages of violent action. It takes place in cube 5 (Figure 8).

Our illustrative scenario centres on the intention of a disparate amalgamation of groups, notably those of an anarchist and anti-capitalist outlook, converging on the City of London in order to engage in violent and large-scale public disorder. These protests are focused on one or more leading sponsors of the Games. The groups' plan, which has been developed via online interaction between a number of individuals, is to cause as much damage as possible to the corporate offices and property of sponsors, as well as attacking other commercial premises and symbolic sites. Several hundred individuals are expected to convene in the City of London for these actions, coming from both the UK and more widely, notably Europe and North America.

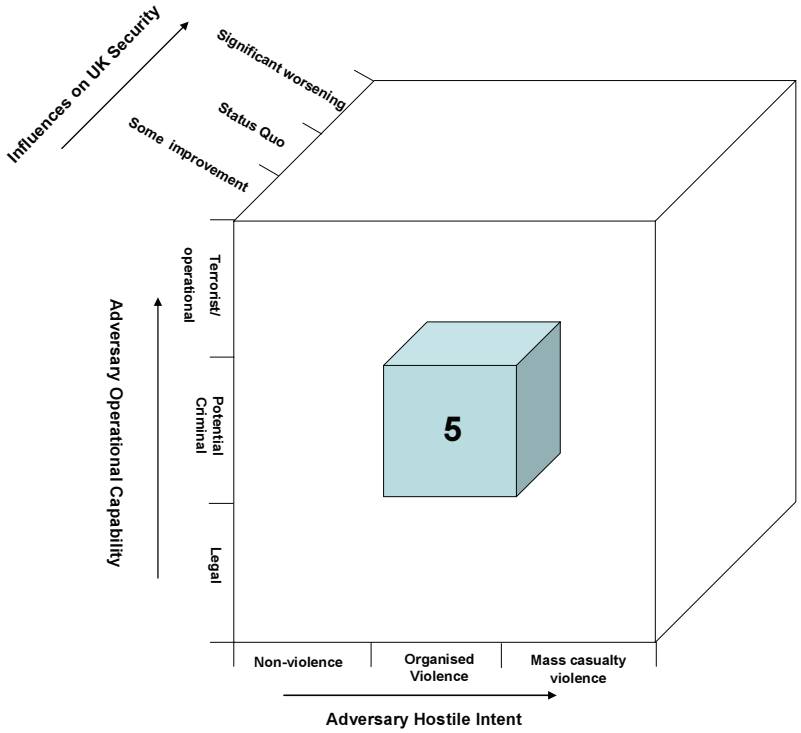

Figure 8. Future security scenario 6

Having constructed these six illustrative scenarios representing a broad range of future security environments, it is now possible to demonstrate the contrasting demands this will place on the UK's security apparatus.

2.4 Assessing the capability implications of potential environments

The RAND study team has constructed a broad list of 41 domestic security capabilities covering the full gamut of security instruments that allow the UK to maintain domestic security, and which will be relevant to pre-empting/responding to security threats during the 2012 Olympics. These range from CCTV and intelligence gathering activities to

Explosive Ordnance Disposal (EOD) and armed military assistance. The study team then made qualitative judgments about the utility of each capability against the six sub-cube scenarios detailed above.

The judgments were made on the basis of the perceived relevance and operational utility of each capability against the nature and severity of the threat. Taking the scenarios in turn, each security capability was evaluated within it and graded as being either as: of critical importance, of importance, of general usefulness, or of limited use. The colour-coding shown in Figure 9 is now used to present the results of this analysis.

Figure 9. Colour coding of security capabilities

In order to arrive at these value judgements, the RAND study team made reference to CONTEST, the Government's long-term Counter-Terrorism Strategy for the UK developed in early 2003.[8] CONTEST is based on four streams:

1) Prevent terrorism by tackling its underlying causes;
2) Pursue terrorists and their sponsors;
3) Protect the public and UK interests; and
4) Prepare for the consequences of an attack.

Each security capability falls naturally under one or more of the CONTEST headings and this provides a basis for judging its utility in any given scenario. It is possible to group the list of capabilities on the basis of these four categories of activity. This helps to facilitate an understanding of whether or not a particular security capability will be relevant and to what degree. The results of this analysis are presented in Figure 10.

[8] For a succinct description of the CONTEST strategy see: Hazel Blears, *RUSI Speech* (22 May 2005) http://press.homeoffice.gov.uk/Speeches/02-05-sp-tools-combat-terrorism

Capability	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6
Explosive Ordinance Disposal (EOD)						
Chemical, Biological, Radiological, Nuclear (CBRN) EOD						
Evidence Gathering and Investigations						
Forensics						
Criminal Justice Process						
Surveillance						
CCTV						
Covert (Area)						
Covert (Individual)						
Overt						
Armed Response						
General						
Suicide Terrorism						
Armed intervention (SWAT)						
VIP Protection						
CBRN First Responders						
Static Weapon/Explosives/CBRN Detection (split)						
Intelligence Gathering						
Human Intelligence (HUMINT)						
Open Source Intelligence (OSINT)						
Signal Intelligence (SIGINT)						
Intelligence Analysis, Assessment and Dissemination						
Communications						
Biometrics						
Other Government Agencies Interaction/ Command and Control (C^2)						
Information/Media Strategy/Operations						
Information Assurance/Security						
Critical National Infrastructure (CNI) Protection						
International liaison						
High Visibility Policing (HVP)						
Crowd Control/Public Order						
Public Disorder/Civil Unrest						
Search & Rescue						
Casualty Reception/Handling						
Mass Casualty Handling						
Decontamination Facilities						
Border Control/Defence						
Military Assistance						
Airspace Control/Defence						
Maritime Control/Defence						
Military Aid to the Civil Power (MAC(P))						
Military Aid to the Civil Authority (MAC(A))						
CBRN assistance						
Physical Security (Area) Transport						
Physical Security (Point) Premises						
Contingency Planning						
Exercise						
Operational C^2						
Specialist Search						
Pre-incident						
Post-incident						
Personnel Vetting						
Community Liaison						

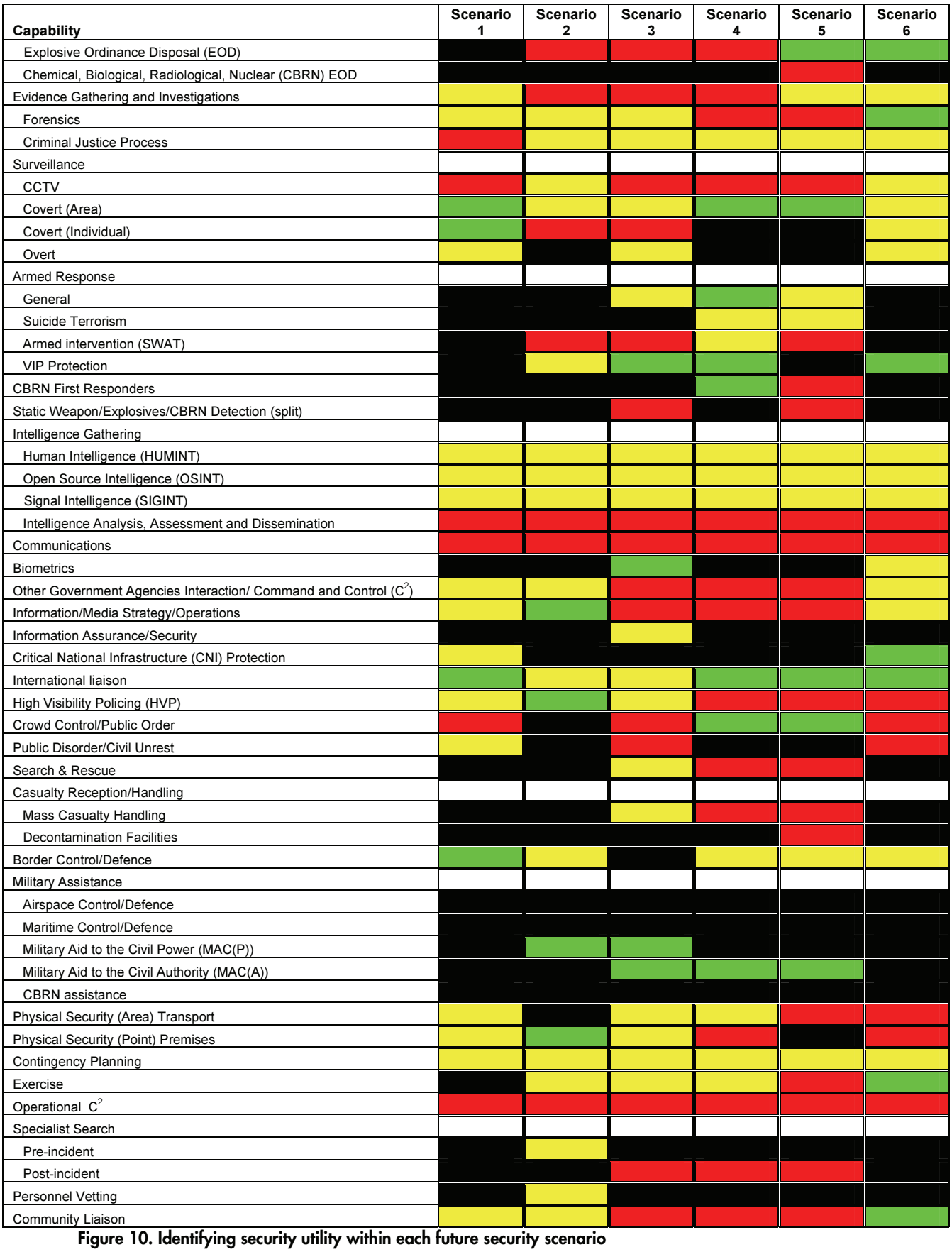

Figure 10. Identifying security utility within each future security scenario

It is important to stress once again the illustrative nature of the six scenarios developed here. This capability analysis represents the widely differing levels of utility each security instrument offers. For example, the results highlight three capabilities that are flagged as 'critical' across every one of the six scenarios: Intelligence Analysis, Assessment & Dissemination; Communications; and Operational command and control. Conversely, the Armed Response capabilities, something that might be expected to figure as being of critical importance, proves only to be of sporadic utility across the range of scenarios considered. Logically therefore, operational preparations and contingency planning should take both of these indicators into account.

2.5 Thinking systematically about security in 2012

It is impossible to predict now the exact nature of the security threat that will impact on the Olympic Games in 2012, but we have demonstrated the feasibility of creating a method to think logically and systematically about the range of potential future security environments that could exist in 2012.

Using the model we have developed will enable us, working in conjunction with security planners, to define a range of future security environments that are considered to be most plausible. It will then be possible to create as many potential scenarios as necessary, with each one having varying implications for current security planning and preparations for future operational response. The implications for a greater or lesser number of operational capabilities can then be mapped across each selected future security environment and the indicative scenarios that have been developed within it.

The model and its accompanying capability assessment process are both highly flexible and infinitely scaleable in their implementation. Both are capable of operating to satisfy high level strategic planning needs or, by utilising much greater detail, meeting those needs at the operational and tactical levels.