Changing Homeland Security:
A Strategic Logic of Special Event Security

Christopher Bellavita

Late one Sunday afternoon two people met in the Utah public safety commissioner's office to talk about Olympic security. One was the commissioner, who also served as the Olympic security commander. The other person was me. We were five months away from the Opening Ceremony for the 2002 Winter Olympics. The commissioner thought it was time for a change, for security planning to transition into security operations. While not quite finished, the Olympic plan was good enough to start using. The purpose of the Sunday meeting was to figure out how to introduce the new strategy to the other members of the public safety security coalition. The date was September 9, 2001. Two days later the Olympic Games became a trivial concern.

Within a few weeks, the embryonic interest in calling off the Olympics had disappeared. The Games became a symbol of national resolve in the face of barbarism. The Olympics would not be cancelled.

The public safety community began to consider what the new terrorism threat meant for Olympic security operations, with the national government leading most of those discussions. Olympic security was now too important to remain exclusively under local control. The first order of business was to examine the Utah Olympic security plan. A variety of federal agencies wanted to make sure there were no flaws in it.

By the time security experts from the national government finished their review, very little in the plan had changed. Aviation support was expanded, access control procedures were tightened, and a few other elements were slightly modified. It was very easy to get money and people – two resources hard to obtain before the attacks. [1]

Even before the Games were over, national leaders praised what was called the "Utah Model" for organizing and planning a major event and recommended it as a best practice for future events.[2] This praise was testament to the thousands of dedicated people who made Olympic security a success. But at a less grandiloquent level, the Utah security organization and plan were in all significant respects based on the same model used for just about every major U.S. special event since the Los Angeles Olympics in 1984.[3] While the scale and complexity of the Olympic Games are unique among international events, there are not many unique ways to structure security for a major special event.

Most American communities will never host a large-scale event, but the lessons learned from providing security at major events can be scaled to other events. The lessons may also help guide homeland security preparedness, particularly in states, regions, and cities. As one Utah public safety agency director put it, homeland security preparedness "feels like we are preparing for the Olympics all over again, we just don't know when they are coming."[4]

WHAT IS A SPECIAL EVENT?

Many communities in the United States host sporting events, concerts, festivals, and other gatherings that have the potential to attract large crowds and dignitaries. These activities are called "special events."[5] The events can also attract criminals and terrorists.

Security has been an integral part of major special events since the 1972 attack at the Munich Olympic Games. In 1980, the United States hosted the XIII Winter Olympics in Lake Placid, New York. Since then, the nation has hosted three Olympic Games, a World Cup, and several dozen other major international sporting and political events. Each of those events received a level of security designed to ensure there would be no repeat of the 1972 Munich attack. Attention to event security increased significantly after September 11, 2001.[6]

For many years, the details of major event security activities were known only within a comparatively small community.[7] The "secrecy" resulted from lack of interest, more than from any concerted effort to keep details hidden. At least one – and often several – after-action reports followed every Olympic or equivalently unique event in the United States since 1980. Almost without exception public safety planners responsible for the next major event ignored those reports.[8]

Before the coordinated terror attacks in Pennsylvania, Virginia, and New York, reinventing the security-planning wheel – while not desired – was accepted as a somewhat minor inefficiency. The contemporary challenge is to better share public safety's collective knowledge to ensure special events remain entertaining and safe.

This article distills the strategic insights of almost twenty-five years of national and international special event after-action reports and experience.[9] The article is written primarily from the perspective of security issues that arise in a major event like an Olympic Games or a gathering of world leaders. My belief is the *strategic*[10] issues and suggestions highlighted here are scalable to special events of practically any size.

There is an aphorism in the Olympic security community: "All Olympics are different. All Olympics are the same." It means, on the one hand, that special events are not paint-by-number enterprises. Each event has its unique security challenges. But the aphorism also means that all Olympic Games – and by extension other special events – have enough security features in common to permit strategic principles derived from prior events to be used as heuristics for future events. The goal of this article is to describe those principles.

The principles are:

1. Start preparing from Day One
2. Understand the life cycle of a special event
3. Anticipate the threat spectrum
4. Write – and live – the security strategy
5. Shape the security landscape

1. START PREPARING FROM DAY ONE

When should event security planning start? Answering this question is leadership's first strategic decision. From one perspective, you can never start early enough. From an opposite view, one can spend entirely too much time planning.

C. Northcote Parkinson's Law says, "Work expands so as to fill the time available for its completion." Security planning for an Olympic Games typically begins six to seven years before opening ceremonies. Planning for the 2004 Democratic National Convention began the same month Boston was awarded the event, twenty months before the convention started.[11] Planning for a parade could begin a few days before the parade starts.

Theoretically, the length of time planning should take is a function of threats, vulnerabilities, resources, the size and complexity of the event, and a security community's experience with special events. But what does that theory mean in practice?

An FBI leader in the 1996 Atlanta Olympics security operation suggested the case for starting early:

> The problem you run into with an event like this is that you can't wait until there's an articulated threat to commit [resources].... So even if there's no threat or no inference of a threat, you've got to go through all the same steps and planning and putting people in place that you would if there were a threat.[12]

The lead security official for the State of Georgia argued for a shorter planning cycle. When asked if he had it to do over again would he have spent years planning for the 1996 Olympics, the official said:

> I would never have told the chiefs [of the public safety departments] anything [about the Olympics] until about six months ahead and then I'd tell them all to rearrange their schedules [and that] I wanted a head count. Then I would have gotten the operational people in, and we would have gone over their head counts, and then I would have told them, "All right, this is your responsibility, this is your venue. I want you to make it safe like you would a sporting event" and maybe add a couple of people to it. And I would have had the operational people identify one operational person for every venue they had, and I would have said, "Now run that son of a bitch and call me when you get a problem, but don't call me till you have problems."[13]

The official was later removed from the planning activity and banished into an operational role that took him out of the state. His perspective on planning was so unconventional that it disturbed national and state security officials enough to pressure the state's governor to replace him.

This anecdote also illustrates the role that stakeholder expectations have on shaping the planning process. Some communities are content planning security for events the way they always have. Other communities cannot seem to do enough planning.

A useful rule of thumb for security planning is to start thinking about core elements of a security plan (i.e., situation or threat, mission, concept of operation, organization, and resources) immediately after the event is announced. This is the Day One Strategy. It can be initiated simply – for example by having a lunch discussion with key public safety partners.[14] Based on the resulting analysis, decide whether the complexity of the event requires extraordinary planning activity, or whether security planning can be incorporated into existing agency functions.

2. UNDERSTAND THE LIFE CYCLE OF SPECIAL EVENT SECURITY

Viewing special events through a life cycle framework helps a leader time strategic interventions. The life cycle perspective suggests when to influence the complexity generated by multiple actors with varied agendas trying to achieve approximately the same global objective: a safe and secure event.

Learn from the Past

It is unusual for major event security to start by identifying what can be learned from the past. People give lip service to the desire not to reinvent the wheel, but when one looks empirically at how security planning begins, there is little evidence that planners or leaders incorporate lessons learned from one jurisdiction into their own.[15]

For some events, like a local fair or an annual special event, institutional memory is frequently a sufficient source of research. If a community has the same major event each year – such as the Kentucky Derby or Indianapolis 500 – lessons from the past are handed down from generation to generation. Major events that travel around the country – the Superbowl, the World Series – have institutionalized the lessons of experience. Those who host unique or infrequent events can also learn from the past.

There is a wealth of information in the United States, going back to the Lake Placid Olympics in 1980, about how to provide security for a special event, about what worked, and about what did not.[16] Typically, the people who are aware of these reports and who read them are either not around when it comes time to plan the event, forget what they read, or are not in an organizational position to implement the recommendations of the reports.[17] Motivated agencies do not have to surrender to obstructions that prevent learning from the past. Seeking access to the accumulated knowledge of public safety agencies with event experience should be the first step for a public safety community responsible for securing an event. Completing this stage properly helps leaders begin to identify potential threats and strategies for countering the threats. (Those two activities are further discussed later in this article.)

Organize To Learn

Depending on the size of the event, existing institutional structures may be suitable for developing security plans. Larger events will require more complex organizational arrangements. Since the late 1990s, agencies have used variations of the Incident Management System as an event security organizing structure.[18]

Major event security generates a unique – and temporary – organizational form. The organization starts with a few people; for the Salt Lake Games it was five. As the event draws nearer, the organization grows. Eighteen months before the 2002 Olympic Games Opening Ceremony, the security group had 150 people in it. When an event starts, the organization expands almost exponentially. At its peak, Salt Lake's Olympic security operations involved more than 11,000 public safety people. A few weeks after the Games were over, the security organization – like a circus leaving town – vanished.

"Form follows function" is one normative guideline for structuring event security. It means the way you are organized should be related directly to what you are trying to accomplish and, as a corollary, to the resources you have available to accomplish the security mission. "Form follows mistake" tends to be the way events are actually organized.[19]

An effective security organization is a dynamic entity that is always *organizing*, and never fully *organized*.[20] It is an organization that actively learns from what is and what is not working, and changes accordingly. Security personnel set up an initial structure for planning and operations. Any deficiencies in the security structure – whether revealed during the planning phase or during operations – can and should lead to structural revisions. Any successes should be replicated where possible in other parts of the organization.

Effective special event security organizations are clear about the mission, the basic principles that govern security operations, the strategy for accomplishing the mission, and the procedures used to plan and execute the security operation. However, it is not unusual for that clarity to be revealed retrospectively, only after the event is over.

Develop the Security Plan

Once the strategies and structures are activated, the detailed and time-consuming work of developing the security plan begins. This stage involves identifying the person or people who will develop the security plan; writing, reviewing and modifying various drafts; and integrating the assorted pieces of the overall plan. Getting ready for a simple event could be one person's additional assignment. More complicated events will require specifically assigned people and resources. (The elements that should be included in a comprehensive event security plan are more than adequately described in other documents.) [21]

In my experience, an event security plan is never finished until the event is finished. The plan continues to grow in comprehensiveness and usefulness. My rule of thumb is to aim for 20% completion of the plan during the first quartile of time available for planning (whether calculated in years, months or days), 40% by the end of the second quartile, 60% completed by the end of the third quartile, and 80% or better as the event arrives.

Obtain Security Resources

This stage is usually the most troublesome part of getting ready for a special event. Special events place demands on public safety agencies whose resources are already stretched.

Because one cannot protect everything, an ideal security plan is based – in theory – on managing risks. Relevant threats and vulnerabilities are identified through the planning process. The steps that can be taken to reduce the risks to an acceptable level are determined. Then resources are obtained by the public safety community and used to reduce the risks.

The reality of event security is not as pure as the standard risk management model assumes. In all but the most major events, there are few additional resources made available by anyone to help secure an event.[22] Since most agencies do not have people standing around looking for work, agencies typically have to meet the event's security requirements by reconfiguring existing resources.

On rare occasions, the event organizers will contribute people, equipment, or money to a security operation. During the 2002 Olympic Games, security costs were covered, in part, by allocating to the public safety budget a portion of each spectator ticket sold. This user-pay model could become a significant source of future event security financing.[23]

Transition to Operation

One of the difficult questions in event security is: when does planning stop and operations begin? A rule of thumb is that planning should be conducted – as much as possible – by the same people within the same structures that will be employed during operations. Transition then becomes organic, and the people who developed the plan are responsible for making it work. For complex events, operations often have to be handed over to multiple agencies and to people who have not been involved intimately with planning. Training, exercises, and the deployment of resources are three activities that signal – and facilitate – the transition phase of the security operation.

Conduct Operations

From a security perspective, perhaps the best thing about special events is they start on a specified day and time. They also have a known end date. This is what distinguishes event security from many other extended public safety operations. Time turns out to be more of an ally in event planning than an enemy.

Once the event starts, public safety does what it does best: makes things happen. Having a security plan brings together trained people with the resources they need to carry out the event security mission. Surprise, uncertainty, and ambiguity are part of the real-world composition of all events. The ability to improvise intelligently around the security plan is the mark of a professional public safety community. This ability is enhanced by the effectiveness of the initial planning strategy and organization. It is honed by the training and exercises appropriate to the magnitude of the event.

In every operation, regardless of complexity and duration, learning occurs. Translating procedures from paper to practice rarely happens without some degree of error. It takes time (a few hours to a few days) to develop a smooth security operation. (Specific ideas about how to make the transition from security theory to security practice are described elsewhere.)[24]

Recover From the Event

The last stage of the event cycle is closing up shop. There are specific activities that mark the end of the security operation – from returning borrowed assets, finalizing overtime, and completing written reports, to recognizing and rewarding the contributions of key people and agencies in the security effort. Not the least of these activities is putting in writing what worked and what did not work – otherwise known as the after-action report (AAR).

As suggested at the start of this life cycle discussion, cultural, organizational, political, and other barriers explain why security providers for one event tend not to benefit from the experiences of their public safety counterparts in other cities and nations. Experience and surveys indicate few people read, understand, or act on information provided in major event after-action reports. But hope persists.[25]

3. ANTICIPATE THE THREAT SPECTRUM

When something significant goes wrong at a special event, there can be lasting economic, political, and social consequences. Decades after the 1972 terrorist attack on Israeli athletes, the name "Munich" can still conjure the grainy video image of the hooded terrorist standing on the balcony at the Olympic Village.

Fortunately, most special events occur without security problems. Occasionally there are incidents, caused by a natural or unintentional hazard such as a hurricane, a lightning storm, or a chemical spill. Problems can also be created by criminal activity, including gang violence and terrorism. Special event security is intended to reduce the risk that something undesirable, from a public safety perspective, will happen.

A basic risk-assessment formula describes risk as a function of threat, vulnerability, and consequences. But, as the Atlanta FBI agent cited earlier said, developing a security plan cannot wait until the intelligence is in. There was no intelligence before the 1996 Centennial Park bombing. In the absence of specific threat information, one can look for guidance from the past about what incidents occurred in previous events.

Christopher Johnson looked at the source and intent of *significant* incidents affecting Olympic Games since Munich in 1972.[26] The results of his analysis are displayed in Figure 1.

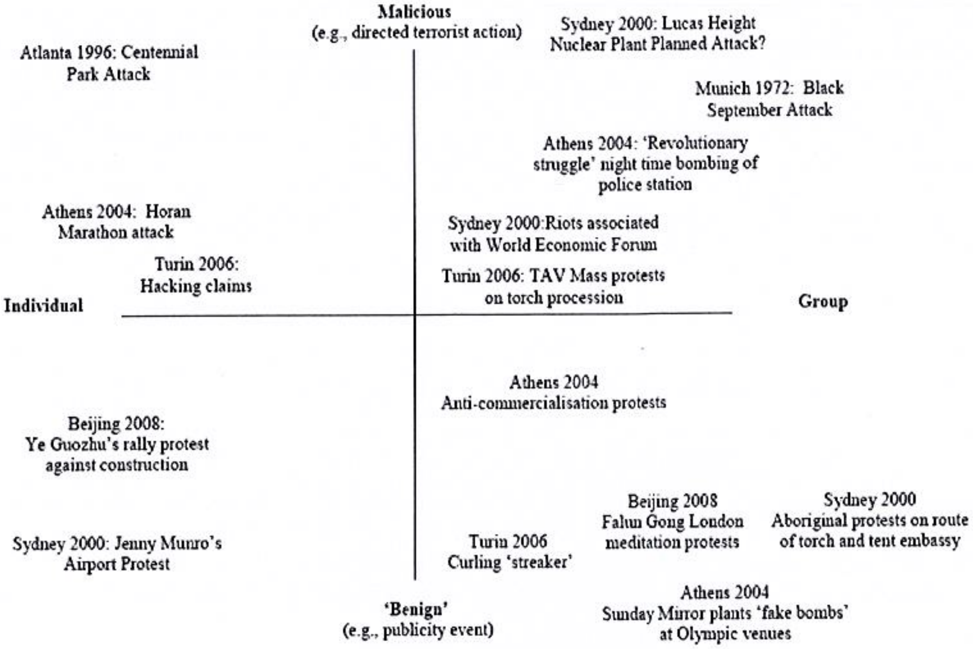

Malicious
(e.g., directed terrorist action)
Sydney 2000: Lucas Height
Nuclear Plant Planned Attack?
Atlanta 1996: Centennial
Park Attack
Munich 1972: Black
September Attack
Athens 2004: 'Revolutionary
struggle' night time bombing of
police station
Athens 2004: Horan
Marathon attack
Sydney 2000:Riots associated
with World Economic Forum
Turin 2006:
Hacking claims
Turin 2006: TAV Mass protests
on torch procession
Individual
Group
Athens 2004
Anti-commercialisation protests
Beijing 2008:
Ye Guozhu's rally protest
against construction
Beijing 2008
Falun Gong London
meditation protests
Sydney 2000
Aboriginal protests on route
of torch and tent embassy
Sydney 2000: Jenny Munro's
Airport Protest
Turin 2006
Curling 'streaker'
Athens 2004
Sunday Mirror plants 'fake bombs'
at Olympic venues
'Benign'
(e.g., publicity event)

Figure 1: Dimensions of Olympic Security

Prior to the 2002 Olympic Games, security planners developed a list of incidents, by frequency, reported for major events in the United States and several other nations[27] since 1972 (Table 1). The list was used as an initial estimate of the types of threats to plan for – to be updated as specific intelligence was obtained. The list was used also to contribute to initial design efforts for Athens 2004 and Turin 2006 security planning.[28] Absent event-specific intelligence, the information in Figure 1 and Table 1 (shown below) can be used to help anticipate the types of threats to be considered in security preparations.

Security-Related Incidents in Order of Probability

1. Hoaxes and threats – such as bomb threats
2. Minor medical injuries
3. Intellectual property rights violations
4. Minor criminal activity – pick pockets, frauds, pranks
5. Vehicle and pedestrian movement problems
6. Fire code violations
7. Weather related problems
8. Public health concerns
9. Demonstrations, some potentially violent
10. Attacks on cyber systems
11. Attempts to extort sponsors
12. Natural disasters
13. Bombings, committed by lone individual rather than by a group
14. Attacks on vital infrastructure
15. Terrorist attack

Table 1: Security Related Incidents at Major Events - From Most to Least Probable

4. WRITE – AND LIVE – THE STRATEGY

Typically, there is little guidance about what the public safety mission is for a large-scale event. For example, here, in its entirety, is the security portion of a contract between the International Olympic Committee (the group that awards a city the rights to hold the Olympics) and a recent host Olympic city:

> Responsibility for all aspects of security is a matter to be dealt with by the appropriate authorities of the Host Country. The City and the NOC [National Olympic Committee] undertake that all appropriate and necessary security measures shall be taken accordingly.[29]

That is all. With little formal guidance – even for an event as large and complex as an Olympics – public safety officials often have to craft their own mission. Effectively, they have three choices in determining what constitutes "all appropriate and necessary security measures":

(1) They can treat the event as something similar to what they do all the time and modify their standard behaviors. This is appropriate when the event is routine or comparatively small.

(2) They can look at the event as something beyond their capability and seek to transfer security responsibility to another entity. This is appropriate when, for example, world leaders hold a politically charged conference in a small community.

(3) Or they can realize there is something unique about what they are responsible for and ask themselves what to do about it. The first step in answering that question is to develop a strategy – a guide to constructing a desired future.

Based on what has worked for past events, an effective strategy will:

1. Unite the security community, especially the senior team, around a coherent and defensible vision.
2. Provide a clear narrative about the role security serves within the larger context of the event and the community where the event will be held. Because there is more to a special event than security, the security story has to show the value public safety adds to the entire event.
3. Establish – and enforce as necessary – security priorities. Most everything public safety does is important, but some security activities are more important than others. Identifying what is important to public safety – and informing stakeholders – helps in the inevitable negotiations that happen during event preparations.
4. Provide guidance based on the priorities. This is akin to a "commander's intent." The guidance gives individuals and work units within the security organization a basis for making independent decisions. The best strategic plans do not identify every contingency. They instead allow individual units to make informed decisions aligned with the strategic vision. The security planners for the Sydney 2000 Games called this guidance the "preferred security position."[30]
5. Consistently emphasize strategic over operational and tactical concerns. The word "strategy" comes from a Greek term that means, "What generals do." Contemporary generals rarely get in the middle of a battle. Event security strategy should stay at the 30,000-foot level and avoid becoming tangled in ground cover.
6. Be put in writing. A surprising number – surprising to me anyway – of event security strategies are not written down. They appear to be transmitted primarily through the oral tradition, meaning someone has to ask what the strategy is.

5. SHAPE THE SECURITY LANDSCAPE

Shaping the security landscape means attending to issues around which conflict occurs during planning and operations. There are few textbook resolutions for these issues. How they are handled will always be context specific. In my experience, they are the enduring strategic issues of special event security. They are what make all events "the same." How these issues are addressed often makes the difference between conducting a professionally mature security operation or an amateur one.

Control: Who is in Charge? (Of What?)

The issue of who is in charge comes up frequently. During the preparation for one of this country's Olympic Games, the vice-president of the United States asked the leaders of the public safety community, "Who's in charge?" The leaders stammered opaquely. [31] For the 2004 Democratic Convention, the official view was the Secret Service was in charge.[32]

"Who is in charge" is only part of a sentence. The complete question should be who is in charge of what? For most events, the specific answer to that question is relatively simple. The answers are found in laws, regulations, and other agreements that determine public safety authorities and responsibilities during normal times. Rarely do those authorities change during a major event, even in the case of concurrent jurisdiction.

Many events display the properties of complex adaptive systems.[33] There are numerous stakeholders, each positioning themselves to achieve their own interests, and at the same time adapting to the actions of other stakeholders. In such a complex system, little of significance is controlled by one group. Instead of asking control questions, the conversation is more constructively directed to clarify who does what, and under what situations. In a well-run security operation, the acronym C^2 means "coordination and cooperation" more than "command and control."[34]

Public Safety Cultures

Complex special events bring together representatives from almost all the public safety disciplines. The reality of different professional cultures having to collaborate and coordinate preparedness activities is a source of conflict. The mix of professional, organizational, and regional cultures can trigger an ethnocentrism that leads to trouble. The impact of culture on event preparedness is not unique to special events in the United States.[35]

The 2002 Olympics brought together almost 100 state, local, federal, and private sector organizations with a stake in security. They represented more than a dozen disciplines.[36] On paper (and in public) everyone worked well together.

But – as in domestic homeland security – most days are spent *preparing* to stop bad guys, and not in an actual battle. There is something about preparing for an event that can activate some of the worst ripples across our culture.[37]

For example, on a bad day getting ready for the 2002 Games, cops were perceived by other disciplines as prima donnas. Firefighters were seen as lazy. Public works was fragmented. Emergency management agencies suffered from an organizational inferiority complex. Private and corporate security personnel were viewed as rent-a-cops. Emergency medical groups were looking for someone to tell them what to do. Public health agencies only seemed able to hold meetings. Infrastructure owners did not want to tell anyone about their vulnerabilities. Everyone was afraid the cops would get more than any other group. All the disciplines were overly sensitive and picked up quickly on any possible slight.

The two-dozen federal agencies that had some stake in Olympic security spent three years in a Byzantine interagency gang war – polite on the surface, intricately vicious in the back rooms. The National Guard and the active duty military component disagreed about almost everything. The Secret Service was reluctant to share anything. The FBI worried another agency would invade its turf. FEMA was fretful it would not get invited to meetings called by the FBI or Secret Service. The U.S. Attorney kept sticking his nose into everyone's business.

Many federal law enforcement agents brought in to help plan the Games looked at Utah public safety as – with some exceptions – a collection of well meaning, but naive hicks. In turn, federal agents were seen as arrogant and inept.

Rural agencies didn't trust their urban counterparts. Sheriffs didn't trust police. Neither trusted the state. No one trusted Washington. And Washington returned the favor.

But that was on a bad day. During the operational period of the Games, almost all of the bickering was put aside to get the job done. When public safety professionals have a vital and immediate mission to do, it takes priority over everything else – including culture.

Inclusion vs. Exclusion

Finding the balance between including and excluding stakeholders is difficult. In the post-September 11th environment, many public safety-related disciplines, and the private sector, want to be a part of security planning for events. There are pro and con arguments for who to include in the overall security planning command structure.

If the security strategy leaves public safety disciplines out of the command or operations structure – public attorneys for example – they can feel excluded and (depending on how it is handled) professionally belittled. There is also the risk of losing access to needed or useful security resources. If the strategy includes within the security structure everyone who has a plausible claim to some public safety interest, the organization can quickly become bogged down in meetings, conflicts, and resource battles.[38]

One solution that has worked for some events is to hold periodic meetings open to representatives of all stakeholders. These gatherings provide people with a chance to learn what is going on. It allows them to provide input into the planning process, as appropriate. It also provides some sense of involvement. The strategy works because many agencies are primarily concerned with insuring their interests are protected, rather than looking for new committees to join or more work to do. Handled clumsily, however, this strategy can also convey a sense that an inner circle is feeding crumbs of information to second tier members of the stakeholder community.

Problem People

Like beauty, a problem person is in the eye of the beholder. In a multi-agency environment, one does not always get to select who works on the security project. It is not unusual for some people involved in an event to put personalities, personal agendas, and ego ahead of the security mission – especially during the planning phase of the activity. Sometimes assigned people do not have the skills, maturity, or commitment the job requires.

Getting rid of problem people is not easy. One may have no choice but to work with them. Ultimately their presence interferes with creating collaborative environments. A senior security planner for the 2000 Olympic Games in Sydney commented, after the Games were over, that the real terrorists were inside his own organization. The lesson: when possible, find a way to quickly remove people from the project who can disrupt collaboration. This does not mean getting rid of people who create conflict. It does mean replacing or marginalizing people who produce difficulties that are not productive for the mission.

Building Trust

Trust is the glue that holds special event security coalitions together. How does one build trust with people and agencies one does not normally work with? Or worse, how does one build trust among agencies that historically do not get along? (In one major event, the chief security planners for two primary agencies had been personal enemies since junior high school.)

It turns out spending time going to tedious meetings, repetitive exercises, and event conferences plays a critical part in building trust among the people who have to make the security operation work. Doing things with people, and doing things often, can create a reservoir of instrumental comity that is sometimes called social capital. The capital generates trust that is used during event operations. It would be good to report that the trust lasts after the event is over. Experience on this point is mixed.[39]

Risks vs. Resources

A major source of conflict in special events is whether to plan primarily from a foundation of *risks* or *resources*. The first time the private sector director of operations for a major event met the chief public safety planner, the director suggested that public safety should develop its plan with an eye toward using the (very limited) resources that were already available. The public safety planner disagreed. He said it was his due diligence responsibility to make sure potential threats were identified and vulnerabilities reduced. If additional resources were needed to do that, they would be found. The relationship between the two men went downhill from that point.

Resource-based logic starts with the view that there is a known, and generally constrained, budget for security. It asks what level of security can be provided for the available resources.

Risk-based logic asks: What is the threat? What are the vulnerabilities? How do we reduce those vulnerabilities? It then assumes that decision makers will obtain the resources needed to reduce vulnerabilities and risk to a level that is politically and professionally acceptable.[40]

Need to Share Resources

Typically, no single agency has enough resources to do what is required during a complex event – and still meet its normal responsibilities. The fact that agencies need to share provides an opportunity for collaboration. It also creates conflicts over who gets to decide how resources are used. Because most public safety leaders tend to be pragmatists, and the mission generally comes first, the conflicts usually are worked out well enough – or at least put on hold – to get the job done. In my experience, regardless of what is written in a formal agreement, the agency that owns the resources always has the final say in how they will be used.[41]

What You are Already Doing and What You Already Have

There is a tendency to view a major event as a unique activity requiring new strategies, structures, and technologies. That perspective is a path to confusion, unfulfilled expectations, and madness. In one major event, the law enforcement commander and a vendor used the event to fund the multi-year development of a complicated personnel-scheduling program. The program graphically portrayed the movement of hundreds of police officers at their posts during a 24-hour period. The program did two things well: it provided a canned presentation of how it *might* work, which was used whenever dignitaries visited the Olympic operation, and it served as the basis for requesting additional development money.

Successful security operations are built on what already is in place. Who is in charge of what today? How do personnel and agencies communicate today? What technology do we use today? Answers to questions like that should drive the foundation of planning and event operations. Compare the answers against an assessment of what is needed to accomplish the public safety mission at an acceptable level of risk. Then seek additional resources to augment the gap. When it comes to arrest procedures, communications, dispatch, fire safety, public works, EMS protocols, or other critical procedures, limit the new. Build on what is already there.

Have a Story But Modify it As Needed

It helps planners and public safety officials if there is a simple and consistent story to tell to the media and people on the periphery of security activities. The story, or narrative, should describe the essential character of the security operation. For example, in one major event, the narrative was: "We anticipate this will be an event everyone will enjoy. We are going to prevent disruptions to the event. We will respond rapidly to any incidents that do happen." The central story served as a conceptual organizing device for public safety officials. It was the core message – the sound bite – officials emphasized during the planning stages of the event.

Every story has a finite lifespan. Typically there are messages that are appropriate during the main phases of security planning: initial organizing, planning, transition, and moving into operations. Effective event planning includes a strategic communication element that can determine when the security message needs to change.

Timing Victories

The process of getting ready for a major event mirrors the issue attention cycle.[42] In the early days of planning, only a few people are involved. Then comes the period of alarmed discovery: the event is approaching and everyone needs to rush to get ready. In this phase, lots of people work on the event, sometimes with an enthusiasm that borders on panic. Next comes the "cost of progress" phase. There is a realization that there are not enough resources or enough time to do everything desired. That leads to a resolve to do "good enough," seeking a balance between what is available and what is acceptable.[43]

Strategic leaders can get the most accomplished, and the most resources allocated, between the alarmed discovery and cost of progress phases of the cycle.

Other Duties As Assigned Creates Burnout

For most events, including major ones like an Olympics, the bulk of the planning work is done by a relatively small group of people. Even though over 11,000 people were involved in the 2002 Olympic Security operations, fewer than two-dozen people did most of the planning. For many small to medium events, it is not unusual for security planning to be the responsibility primarily of a single person. It is also rare for event planners to be relieved of their other duties. Planning becomes one of those "other duties as assigned" activities.

If the security operation is treated seriously, people responsible for security planning are among the best people in the agency. They are given the planning responsibility because they have already demonstrated their competence. As a result, these already overworked people can burn out long before the event arrives.

Single Points of Failure

Information or skills critical to security's success should not reside solely in one person or agency. Agencies using one planner should be aware that overburdening a security planner makes that planner a potential single source of failure for the entire operation. It makes sense, for several reasons, to have at least two planners who each know what the other knows. If something happens – which it often does – causing an agency or key individual to no longer be involved, the remaining person or agency does not have to start from the beginning. As illustrated next, relying too much on a specific technology can also create a single point of failure.

New Technology

One hour before the first event at a 1994 World Cup venue, a temporary bridge collapsed. Public safety personnel from four agencies rushed to the scene to see if anyone was trapped in the debris. At the start of their shifts they had been issued new radios to allow them to talk with each other. Many of the officers discovered, as they responded to the scene, that they did not truly understand how to use the new radios. Conceptually similar scenes have been repeated in event after event.

New technology is a source of both promise and anguish at major events. The more international attention the event receives, the greater the likelihood public safety leaders will be tempted by the marketing messages of vendors. The experiential evidence about the usefulness of innovative technology (or technology that is new to a jurisdiction) at major events is fairly one-sided. The technology rarely performs as promised or as designed. Sometimes the fault rests with the technology. Other times – as in the radio example – the problem is user error. When existing technology can get the job done, it should be used. It makes little sense to train people for a system they will use for, say, one month, if they already have something that will work.

Communication Will Be a Problem

A few minutes before 1:00 AM on July 27, 1996 a security guard noticed an unattended backpack under a bench in Atlanta's Centennial Park. He informed a police officer, who started moving people away from the object. Several minutes later, a man dialed 911 and said, "There is a bomb in Centennial Park. You have thirty minutes." At 1:20 AM, a police officer reported an explosion at the Park. Two people died as a result of the explosion; over 110 people were injured.

The problems associated with efforts to get the information about the bomb threat to the right people are legend in the special event security community.[44] Even if communication had worked perfectly, here is what would have had to happen within the communication protocols created for the Games: (1) The Atlanta **dispatcher** who received the 911 call would notify (2) the **Atlanta Agency Command Center** (ACC). The person who took the call at the ACC would notify (3) the **state representative** in the ACC (because Centennial Park was a state controlled venue). The state representative would notify (4) the **State Olympic Command Center**. The person who took the call in the state center would notify (5) the Centennial Park **venue commander** who would then notify (6) his **officers**.

If, in a hypothetically "perfect" world, each communication took only three minutes, the message about the bomb threat would take almost twenty minutes to get to the officers who needed to act on the information. Nine of those police officers – unaware of the call – were moving people away from the unattended backpack. All were hit by shrapnel when the bomb exploded, twenty minutes after the bomb threat.[45]

The Atlanta Olympic communication protocol was the result of political, organizational, and technological factors of that particular event. While there is much to critique about that incident, the focus here is on communication. The 911 call was made from a payphone outside Centennial Park. Yet the call had to be routed all over the city to transmit a message to someone less than 100 yards away.

A lesson from almost every training exercise is "communication was a problem." The same lesson emerges from major event experience. Even with efficient protocols, communication difficulties are certain to occur during a special event. And the more agencies involved, the greater the likelihood of problems.

Utah had six years to plan its Olympic communication system. Yet still they encountered obstacles, with both the technology and sociology of communication. Major events require communication among agencies that are not used to working with each other. It takes time to learn how to communicate effectively.

During the seventeen days of the Games, the communication network processed 8.5 million calls, almost 350 calls every minute of the operational period. Most of the time the system worked well. But even with six years of planning, Department of Defense and Secret Service radios interfered with each other. The Olympic Organizing Committee sold some of its frequency to an international ski team and the frequency interfered with public safety communications. Encrypted radios had a difficult time communicating with non-encrypted radios. Some agencies used coded voice communications; others used plain English. Some disciplines used radios for succinct communications; others used the radio to chat. Those are just a few of the *radio* communication problems. There were analogous technological and human factors difficulties with video, telephone, internet, and other modes of communication. Overall, communication was one of the success stories of the 2002 Olympics. But still there were problems.[46]

Paradoxically, events can also generate more information than agencies are used to receiving. In such an environment it can be difficult to discern what is signal and what is noise. After-action reports recommend installing, testing, and practicing with communication equipment and protocols as early and as frequently as possible. Nonetheless, strategic leaders should plan for the inevitability of communication problems and ensure redundancies exist to allow the transmission of critical information.

Plan on Everything Changing

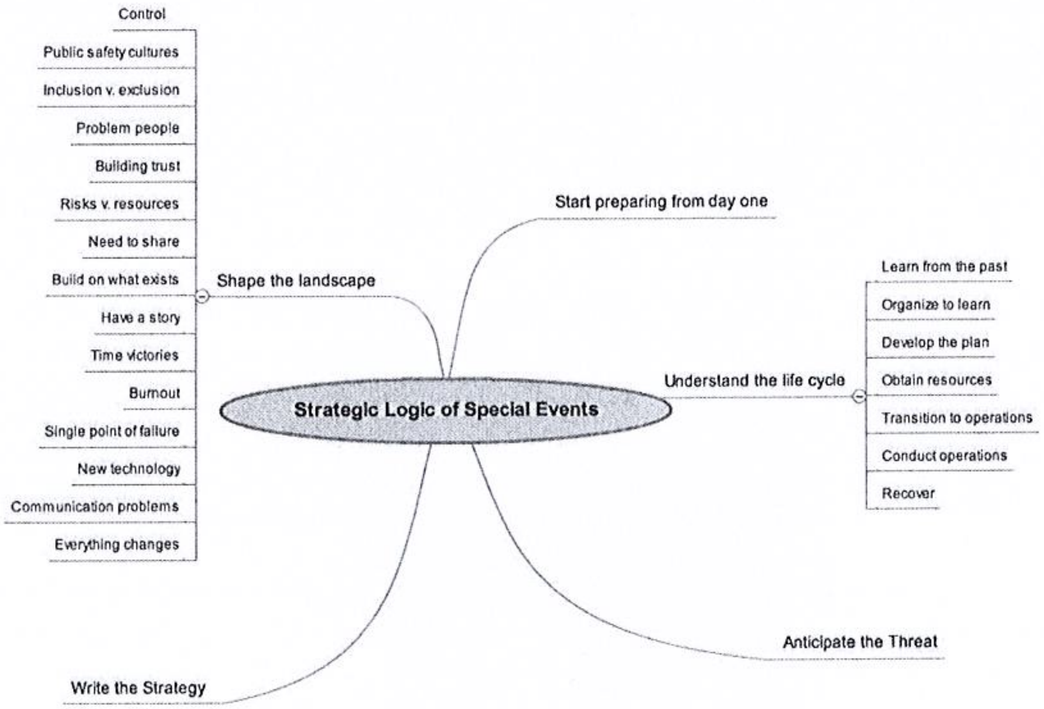
As one after action-report delicately phrased this issue, "Commitments [made]... to public safety agencies were not always dependable." This applies to people, procedures, resources, and promises. One may have an image that for a major event, at some point the plan is completed, and then operations begin. But special event planning is never finished. There may be documents and charts and PowerPoint presentations that describe "The Plan," but for many events there are significant differences between what is in the plan and what is on the ground. Venues, schedules, personnel, and other features of the event change daily. Some of these changes have significant impacts on security. The changes can be a source of conflict. Strategic leaders should not assume things will happen the way they are told they will happen. For the important things, public safety should prepare to do for itself what others say they will do for them.

CONCLUSION: PREPARING FOR THE NEXT EVENT

Major special events create complex systems. In such systems actors continuously adapt to each other and to the unpredictable vitality of ambiguous and turbulent environments.[47] As a result, success measures for event security are characterized less by reference to such terms as efficiency, stability, standard operating procedures, and control, and more by such words as effectiveness, resilience, rules of thumb, and cooperation.[48] In this respect, having to prepare for special events appears similar to the environment faced by homeland security leaders.

Figure 2 (below) summarizes the elements of a special event strategic logic.

FIGURE 2: The Elements of a Special Event Strategic Logic



From a public safety perspective, two guidelines emerge as the primary strategic lessons from previous events: (1) Be steadfast on the issues that are important to public safety and (2) Be flexible about everything else.

The utility of these guidelines may also be relevant to homeland security.

Christopher Bellavita teaches in the master degree program at the Naval Postgraduate School in Monterey, California. An instructor with twenty years experience in security planning and operations, he serves as the Director of Academic Programs for the Center for Homeland Defense and Security. Prior to joining NPS, Dr. Bellavita was the executive director of the Utah Olympic Public Safety Command. He received his PhD from the University of California, Berkeley. Dr. Bellavita can be contacted at cbellavi@nps.edu.

[1] *Utah Olympic Public Safety Command After Action Report* (Salt Lake City, Utah, November 2002), Chapter 3, "Olympic Games and Public Safety," 6. Available from the author, cbellavi@nps.edu.

[2] For examples, see "Inside the FBI: 2002 Olympics," washingtonpost.com, January 17, 2002, http://discuss.washingtonpost.com/wp-srv/zforum/02/fbi0117.htm. Similar comments were made by FBI director Robert S. Mueller, (http://www.fbi.gov/pressrel/speeches/slc.htm) and Attorney General John Ashcroft (http://www.usdoj.gov/opa/pr/2002/January/02_ag_047.htm). Praise for the Utah Model can also be found in the Department of Homeland Security, *National Strategy for Homeland Security* (2002), A-3. After the 2004 Athens Olympics, the Greek Minister of Public Order suggested that the Hellenic model was also a best practice. See Dr. George A. Boulgarakis, "The Olympic Security Model As A Pattern Of International Cooperation In Order To Confront New Threats," April 11, 2005, http://www.greekembassy.org/Embassy/content/en/Article.aspx?office=3&folder=815&article=14973.

[3] Los Angeles Police Department, *Olympic After Action Report* (Los Angeles California, n.d., but written in late 1984). For a similar observation, see Ester Scott, "Security Planning for the 2004 Democratic National Convention (A)," Kennedy School of Government Case Program, C16-05-1807.0 (2005), 6: "Sheafe [the lead agent for the Secret Service] could refer as well to previous NSSEs and his own experience on the presidential detail for ideas. 'I can look and see the subcommittees they had for the DNC in 2000 ... and I can see the subcommittees they had for the Olympics. And I know that if I go on an advance for the president, I need support from all these different groups, so it's basically the same model."

[4] Scott A. Behunin, "Homeland Security Advisory System" (master's thesis, Naval Postgraduate School, 2004), 31.

[5] For an excellent discussion of special events, see G.B. Jones "Towards A Strategic Approach To Special Events Management In The Post 9/11 World," (master's thesis, Naval Postgraduate School, 2005). Jones writes that the FBI defines a special event as "A significant domestic or international event, occurrence, circumstance, contest, activity, or meeting, which by virtue of its profile and/or status represents an attractive target for terrorist attack." (Chapter 2, page 10). In 2005, the FBI treated significant special events as falling within one of three categories: major sporting events, Politically Charged Special Events (PCSEs), and National Special Security Events (NSSEs). In *Special Events Contingency Planning Job Aids Manual,* (Washington, D.C.: FEMA, March 2005), 1-1, the Federal Emergency Management Agency (FEMA) defines a special event as "... a non-routine activity within a community that brings together a large number of people. Emphasis is not placed on the total number of people attending but rather on the community's ability to respond to a large-scale emergency or disaster or the exceptional demands that the activity places on response services. A ... special event requires additional planning, preparedness, and mitigation efforts of local emergency response and public safety agencies."

[6] Scott, "Security Planning for the 2004 Democratic National Convention (A)," 1.

[7] For two exceptions, see *Managing Major Public Events: A Planning Guide for Municipal Officials, Law Enforcement, Community Leaders, Organizers, and Promoters*, (Washington, D.C.: U.S. Department of Justice, Community Relations, November 2000) and FEMA, *Special Events Contingency Planning Job Aids Manual*,.

[8] Generally on this point, see *Utah Olympic Public Safety Command After-Action Report*, Chapter 38, "Why After Action Reports Are Ignored;" Amy K. Donahue and Robert V. Tuohy, "Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We Can Learn Them," *Homeland Security Affairs* 2, no. 2 (July 2006) http://www.hsaj.org/?article=2.2.46;

and Chris W. Johnson, "Contingency Planning for 2012 Olympic Venues," (no date), http://www.dcs.gla.ac.uk/~johnson/papers/Olympics/Chris_Johnson_Olympics_v2.pdf.

[9] The information in this document draws significantly from unpublished special event security after-action reports from the events listed below. Dozens of now anonymous people spent hundreds of hours collecting information for and writing the reports. Thank you for your work. The reports were supplemented by planning documents, interviews, and personal experiences. The events from which the information in this article is derived include the 1984 Olympic Games in Los Angeles; 1987 Pan American Games; 1990 Goodwill Games; 1992 World University Games; 1992 Barcelona Games; 1994 World Cup; 1994 Lillehammer Olympic Games; 1996 Atlanta Olympic Games; 1998 Nagano Olympic Games; 2000 Sydney Olympic Games; 2002 Salt Lake City Games; and 2004 Athens Olympic Games. Please contact me at cbellavi@nps.edu if you would like additional information about specific after action reports.

[10] I use *strategic* in this paper to refer to leadership issues that affect the general direction and character of event activities. The paper is not about operational or tactical issues, although references are provided elsewhere in this document for any reader interested in more operational information.

[11] Scott, "Security Planning for the 2004 Democratic National Convention (A)," 7.

[12] John Buntin, "Security Preparations for the 1996 Centennial Olympic Games (B)," Kennedy School of Government Case Program, C16-00-1589.0, 17. This case study provides the most realistic and comprehensive discussion I have seen about the political dynamics of planning for a major event.

[13] Ibid, 9.

[14] This is how planning for the Salt Lake City Olympic security began, a few days after the city was awarded the bid. For the 1994 Barcelona Olympics, much of the strategic planning took place over lunch. In Atlanta it was at a downtown bar. In Utah it was at breakfast. But I digress.

[15] This does not mean efforts are not made to learn from the jurisdictions that held a specific event in the past. Visiting an event you will have in the future – like a Superbowl, World Series, or Olympics – is a well-honored tradition in the event security community. But for reasons discussed in *Utah Olympic Public Safety Command After Action Report,* Chapter 38, "Why After Action Reports Are Ignored," those efforts to integrate lessons rarely succeed.

[16] Before the Department of Homeland Security's lessons learned web site (llis.gov), there was no central repository for these documents. The llis.gov site has begun to collect key after-action reports. Other reports, if they exist, are buried deep in agency archives, or are in the personal files of individuals involved in those events.

[17] Interviews I conducted after the 2002 Olympics indicated perhaps several dozen people knew after-action reports from prior events existed. A smaller number read one or more of the reports. Fewer than five people remembered anything they had read, or acted on something they had read.

[18] I first encountered the use of the incident command system (ICS) for events during preparations for the 1999 World Alpine Ski Championships. See Greg Morrison and Joseph Airey, "Special event safety and security: protecting the world alpine Ski Championships," *FBI Law Enforcement Bulletin* (April, 2002) for details, along with information about difficulties they encountered using ICS. More recently, security preparations for the 2008 U.S. Olympic Track and Field Trials in Eugene, Oregon are using the ICS structure as an organizing and operations principle.

[19] This concept comes from Henry Petroski, *The Evolution of Useful Things* (New York: Alfred A Knopf, 1992).

[20] This insight comes from Karl E Weick, *The Social Psychology of Organizing,* 2nd Ed. (McGraw-Hill Humanities/Social Sciences/Languages, 1979).

[21] See *Utah Olympic Public Safety Command After Action Report*; Department of Justice, *Managing Major Public Events*; FEMA, *Special Events Contingency Planning Job Aids Manual*; and "Olympic Security Review Conference" (October 2003), www.markle.org/downloadable_assets/2002olympics_security.pdf.

[22] Even National Special Security Events do not guarantee any new money will be appropriated specifically for the subject event's security. See Scott, "Security Planning for the 2004 Democratic National Convention (A)," 4.

[23] Christopher Bellavita, "Fans should pay for security at the Trials," *Register-Guard,* Eugene, Oregon, March 5, 2006. For one view of how this strategy came about, see Mitt Romney (with Timothy Robinson), *Turnaround: Crisis, Leadership and the Olympic Games.* (Washington, D.C.: Regnery Publishing, 2004), 294-295. [In what must be a misprint in Romney's book (p.296), he writes Utah's public safety commissioner had been a sheriff in southern Utah prior to becoming commissioner. It is a distinction that may matter mostly to law enforcement, but the commissioner had been a police chief, not a sheriff.]

[24] See *Utah Olympic Public Safety Command After Action Report*, especially Chapters 5 through 15, and 22. Also, "Olympic Security Review Conference."

[25] See the epilogue in Scott, "Security Planning for the 2004 Democratic National Convention," especially pages 3-5

[26]Johnson, "Contingency Planning for 2012 Olympic Venues," 9.

[27] The data for this list – intended more to guide approximations than to be precise – was derived from the 1992 Barcelona Olympics, the 1994 Lillehammer Olympics, the 1994 Word Cup, the 1996 Atlanta Olympics, and the 2000 Sydney Olympics. Incidents at events prior to 1992 (such as the Los Angeles Olympics, Lake Placid Games, World University Games, Pan American Games, and Goodwill Games) were also included. The information was developed by interviewing security personnel involved in the events, by examining after action reports and (for World Cup 1994 and Atlanta 1996) by reviewing detailed security incident logs.

[28] From conversations between the author and senior law enforcement officials in Athens and in Turin.

[29] The language comes from an unpublished document in the personal archives of a (now former) public official who requests that his name not be used.

[30] For the 2000 Olympics, the New South Wales police developed the "preferred security position" that follows. As the carefully selected name suggests, it is the position law enforcement "preferred," but it also signaled to stakeholders that the police would be open for discussion around those principles. The principles (from an unpublished 1999 New South Wales police Olympic planning document) were:

1. Protect the integrity of international entry and accreditation processes to ensure they are consistent with security and Australia's existing policies.
2. Ensure all accredited persons are subjected to appropriate background checking procedures by government authorities.
3. Restrict sensitive areas to accredited persons. Amongst other measures, some form of perimeter fencing should be in place around all venues and sites.
4. Sanitize all Olympic venues and sites for the presence of explosive devices after "lockdown" of the venue by [the Olympic organizing committee] and re-sanitize as required on the basis of specific risk.

5. Impose random, but carefully targeted, screening procedures using metal detectors and searches of hand carried items, under the supervision of New South Wales Police Officers, for all spectators entering Olympic venues and sites.
6. Apply more thorough checking procedures of all people and items entering higher risk areas such as the Olympic Village.
7. Apply strict and consistent zone controls within each venue and site, aimed primarily at the protection of the Olympic Family and VIP's.
8. Impose strict and consistent controls on the entry of vehicles and commercial materials into all Olympic venues and sites.

[31] Buntin, "Security Preparations for the 1996 Centennial Olympic Games," 11 and 12. The case study, written a few years after the event, suggests a more articulate answer was provided to the vice-president. The story told by participants at the meeting once they returned to Atlanta supports the "stammering" assertion. For another view of this meeting, see Mitt Romney's May 2004 testimony to the U.S. Senate Committee on Commerce, Science, & Transportation, available at http://www.iwar.org.uk/homesec/resources/olympic-security/romney.htm. Contrary to Buntin's report, Romney believed the meeting with Vice President Gore took place in Atlanta, not Washington, D.C. Romney uses the story to support his notion that for a major event under high threat conditions "you want someone who can tell you that they are responsible for the overall effort." For an FBI view of how security authority was shared in the 2002 Olympics, see "Inside the FBI: 2002 Olympics," *washingtonpost.com*, January 17, 2002, http://discuss.washingtonpost.com/wp-srv/zforum/02/fbi0117.htm.

[32] "There was no argument about who was in charge," says Carlo Boccia, director of the Mayor's Office of Homeland Security, "because that was designated—the Secret Service was in charge." In practice, the USSS appears to have been "in charge" in only one of eight security zones. Scott, "Security Planning for the 2004 Democratic National Convention (A)," 9.

[33] For a helpful review of complexity theory and its application to how organizations function, see Philip Anderson, "Complexity Theory and Organization Science," *Organization Science, Special Issue: Application of Complexity Theory to Organization Science* 10, no. 3, (May - Jun., 1999): 216-232.

[34] In my view, this is a primary lesson from the Democratic National Convention experience. See Scott, "Security Planning for the 2004 Democratic National Convention," 3-4.

[35] For an Australian example, see the Sydney Olympic comment, in the "Problem People" section that follows. Planners from Barcelona, Turin, and Athens reported similar stories to me about conflicts rooted in professional and jurisdictional cultures. Where state and local agencies in the United States may disparage Washington D.C. agencies, police officers in Turin spoke the same way about officials from Rome, as in "Watch out, here come the know-it-all Romans" (a phrase that probably sounds better in Italian).

[36] The disciplines included fire, police, emergency medical, emergency management, public works, public health, physicians, military, private sector, intelligence analysts, EOD, aviation, and other scientific disciplines (chemists, structural engineers, electronic specialists, communications specialists).

[37] Ester Scott reports a somewhat different outcome in Boston. "We jokingly refer to the Democratic National Convention here among the law enforcement community ... as the summer of love," one person reported. "Security Planning for the 2004 Democratic National Convention," 4.

[38] There were sixty agencies on the Atlanta Olympics security governing body. As one participant noted, "[Once] you get beyond about five or six or seven people, it's not a policy-making group anymore. It's a convention...." Buntin, "Security Preparations for the 1996 Centennial Olympic Games," 11. The proliferation problem persists a decade later, but now with command centers.

There were twenty-nine "command centers" for the Democratic National Convention. Scott. "Security Planning for the 2004 Democratic National Convention," 3.

[39] After the 2002 Salt Lake Olympics, the federal agency representatives who used to call their state and local counterparts two and three times a day, stopped calling. Everyone had other work to do – other projects to work on. The city's police and fire chief – who shared space in the same building – meant to have lunch together, but never quite got around to it. One needs a reason to spend time outside one's culture. For projections about the impact on interagency relations of the DNC event, see Scott. "Security Planning for the 2004 Democratic National Convention," 4.

[40] For how this issue was handled in Boston, see all three parts of Scott's "Security Planning for the 2004 Democratic National Convention."

[41] For example, even though the Department of Defense might support an event with aircraft or explosive ordnance disposal people and equipment, DoD must always agree how those resources will be used. The same goes for a county or city that might provide its police officers to assist with crowd control. Those officers almost always remain under the control of the owning agency's command staff and operational procedures. Even in a sharing environment, those with the "gold" – i.e., resources – tend not to relinquish control.

[42] Anthony Downs, "Up and Down With Ecology: The 'Issue-Attention Cycle'," *The Public Interest* 28 (Summer 1972): 38-50.

[43] A more cynical model about the phases of a special event (borrowed from the project management world) echoes the issue-attention cycle: 1. Enthusiasm, 2. Disillusionment, 3. Panic, 4. Search for the guilty, 5. Blame the innocent, 6. Reward the uninvolved.

[44] "FBI defends Olympics bomb probe; 911 transcript shows delay," August 9, 1996, http://www.cnn.com/US/9608/09/olympics.bomb.911/. Johnson, *Contingency Planning for 2012 Olympic Venues*, 2-3; and Buntin, "Security Preparations for the 1996 Centennial Olympic Games," 7- 15. For additional information about this incident, see the numerous historical links available at http://www.washingtonpost.com/wp-srv/national/longterm/bombing/bombing.htm.

[45] Joan Kirchner, "How Olympic Bomb Was Found," July 27, 1996, http://www.washingtonpost.com/wp-srv/national/longterm/bombing/stories/found.htm.

[46] *Utah Olympic Public Safety Command After Action Report*, Chapter 15, "Communications."

[47] Anderson, "Complexity Theory and Organization Science," 216-232.

[48] David Snowden, "Antonyms for sense-making," *Cognitive Edge*, http://www.cognitive-edge.com/2006/09/antonyms_for_sensemaking.php.

This page is intentionally blank

This page is intentionally blank