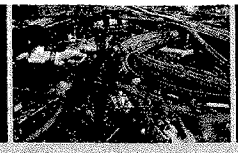
Securing High Risk Events



Big Dig Blues

Anthrax Alert Lessons

June 2005 • Vol. 2, No. 6 • $5.95 USD

HSToday

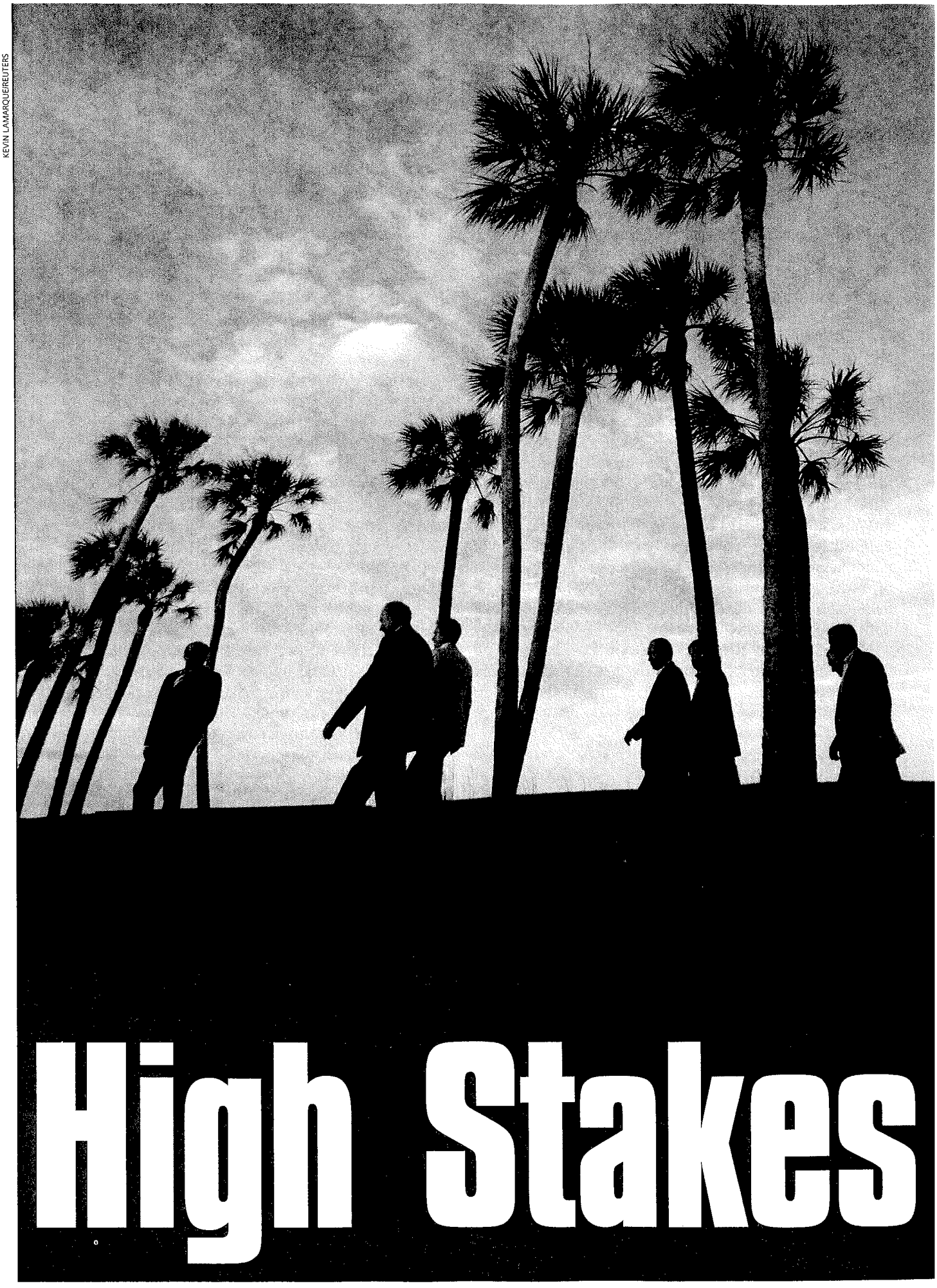
Insight & Analysis for Homeland Security Policymakers

The Border Issue

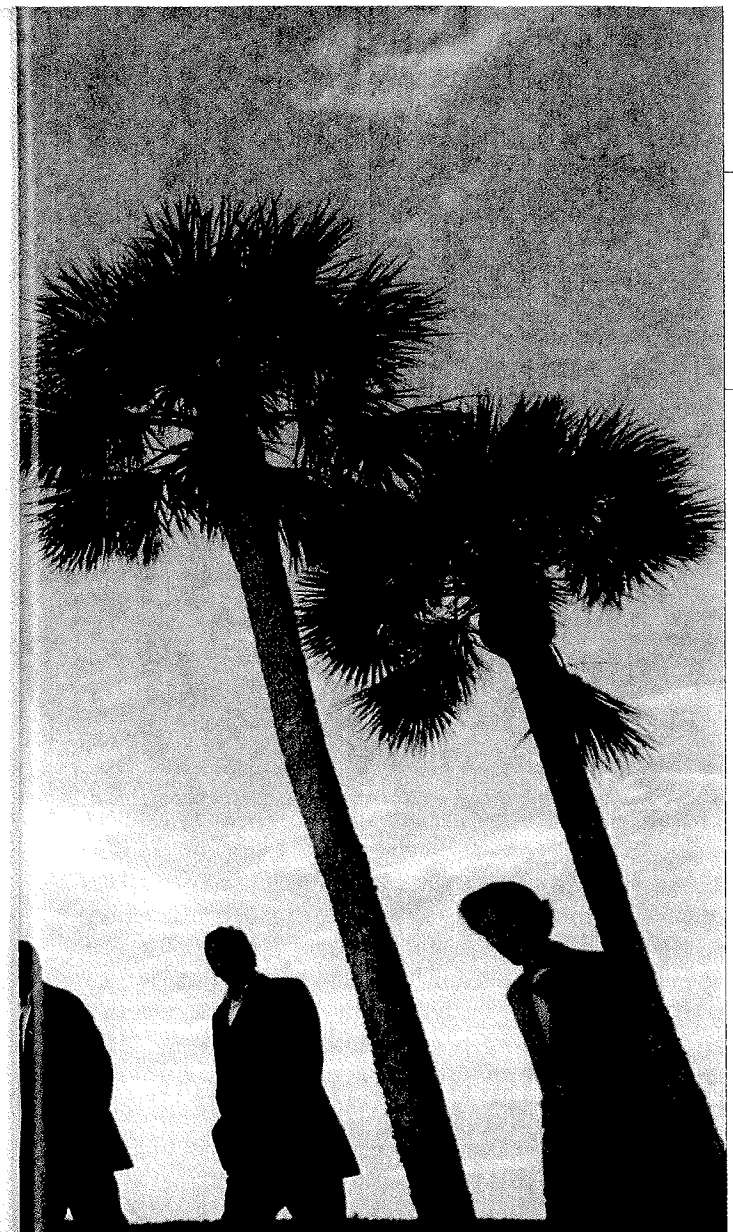
From Mexico City to Ottawa— the st… on A… borders

www.HSToday.us

KEVIN LAMARQUE/REUTERS



High Stakes



The G8 summit leaders (left to right) Italian Prime Minister Silvio Berlusconi, Canadian Prime Minister Paul Martin, British Prime Minister Tony Blair, Russian President Vladimir Putin, European Commissioner Romano Prodi, Irish Prime Minister Bertie Ahern, US President George W. Bush, French President Jacques Chirac, German Chancellor Gerhard Schroeder, and Japanese Prime Minister Junichiro Koizumi walk along the beach at Sea Island, Ga.

As big events become bigger and more complex, so do the challenges in securing them—and so does the technology assisting their protectors.

BY PHILIP LEGGIERE

Security

AFTER MONTHS OF ANXIETY ABOUT POTENTIAL BIOTERROR INCIDENTS, THE G8 SUMMIT AT SEA ISLAND, GEORGIA, LAST JUNE WAS PROCEEDING SMOOTHLY. DEMONSTRATIONS IN THE VICINITY OF THE MEETINGS WERE TURNING OUT TO BE SMALLER THAN EXPECTED, AND THE SCORES OF INTERNATIONAL DIGNITARIES ATTENDING THE EVENT HAD SAFELY MADE THEIR WAY TO THE PROCEEDINGS. SO FAR, SO GOOD.

Shortly after the summit began, however, the mood quickly and ominously shifted, when rumors spread that one or more very high-profile dignitaries had begun complaining of what appeared to be food poisoning.

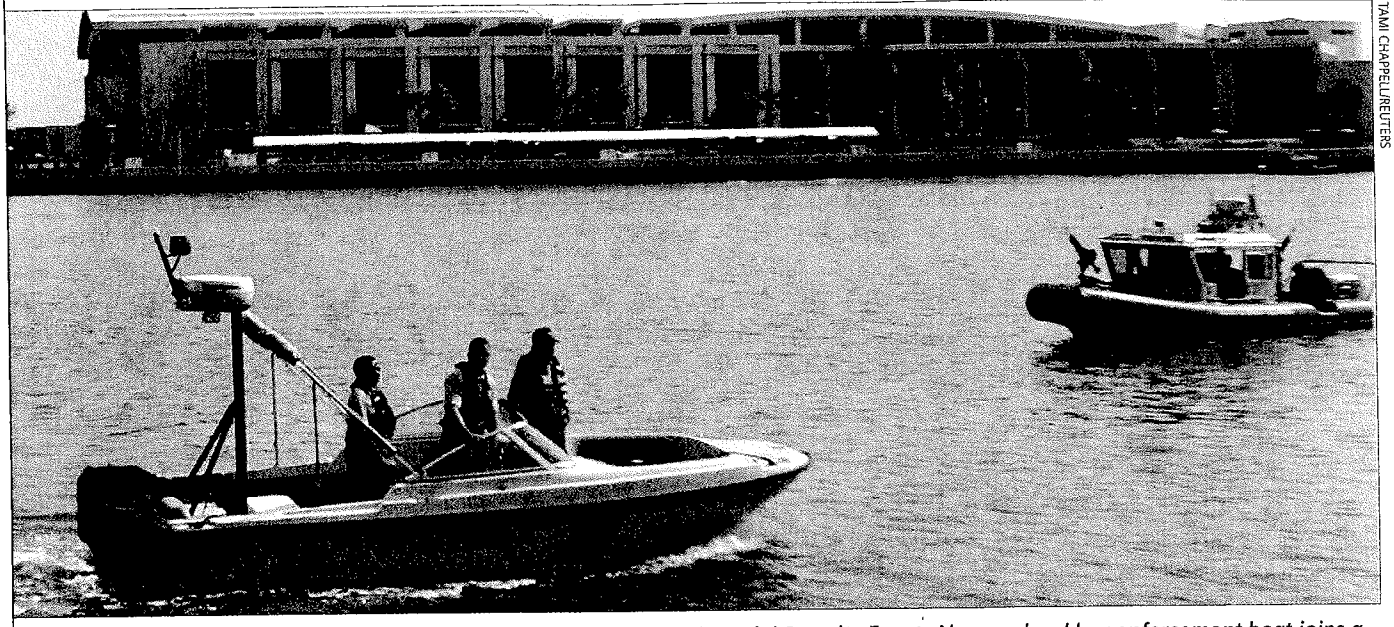
"It was the type of incident that no one would have batted an eyelash at 10 years ago," Todd Stout, founder and CEO of Stout Solutions, a California-based developer of bio-monitoring and data analysis tools, told *HSToday*. "But in a post-9/11 climate, when terrorism is on everyone's mind, all it takes is a small thing like this and rumors can escalate in a flash into full-scale panic about the possibility of a wider outbreak."

Fortunately, officials at the Georgia Department of Human Services, Division of Public Health, and an expert team from the Center for Public Health Preparedness and Research at Emory University in Atlanta, had found a way ahead of time to run what they termed a "reality check" in such instances and separate false alarms from real public health concerns. Using technology designed by Stout Solutions, officials were able to monitor all emergency medical and 911 call data throughout the region in real time. They were thus able to ascertain without a doubt that no pattern of food-poisoning incidents was emerging and stop an incipient panic in its tracks.

THE ORIGINS

The G8 food poisoning scare turned out to be a blip during an ultimately safe, secure summit. Indeed, even the original reports of food poisoning turned out to be untrue. But it tellingly illustrates the changed terrain in which security planning for major events has to operate in a post-Sept. 11, 2001, world.

"It's common sense that big events make inviting targets," explained US Secret Service spokesperson Tom Mazur, "especially when you have massive numbers of people, including dignitaries and/or VIPs, in attendance. That's always been the case. But in the modern age, the dangers are magnified. With mass media coverage, a presidential inauguration, a Super Bowl and a state funeral service are



TAMI CHAPPELL/REUTERS

Both land and water approaches require vigilance during a National Special Security Event. Above, a local law enforcement boat joins a US Coast Guard boat in patrolling the Savannah River during the G8 summit in June 2004.

now global events on a global stage seen by billions. When you put global media and the threat of global terror together, it really amplifies the stakes."

In recognition of these new challenges, the administration of President Bill Clinton in 1998 created a new security category called the National Special Security Event (NSSE) to cover the requirements of securing such mega-events. In May of that year, Clinton issued Presidential Decision Directive 62, a classified document mandating better coordination between different federal antiterrorism and counterterrorism assets. In December 2000, the concept of the NSSE was authorized and formalized by Congress as part of the Presidential Protection Act of 2000.

The NSSE acronym designates the highest-level of special events as determined by the Department of Homeland Security (DHS). Once an event has been designated an NSSE, a series of security procedures and protocols are initiated involving close coordination between federal agencies and local officials. Lead strategic planning and operational responsibility in an NSSE lies with the US Secret Service. The Federal Bureau of Investigation (FBI) takes the role of lead investigator of criminal activity, and the Federal Emergency Management Agency (FEMA) manages emergency response in the aftermath of a terrorist attack.

Although the Secret Service will not divulge details of the specific methods and means associated with NSSE operations, a sense of the complexity and scope of federal agency commitments involved in an NSSE can be gleaned from the security Fact Sheet for the June 2004 G8 summit released by DHS. Participants in that event included:

- The US Bureau of Immigration and Customs, which deployed special agents and mobile command vehicles to Savannah, Brunswick and Sea Island, Georgia.
- FEMA, which provided multiple disaster response teams, capabilities and assets, including urban search and rescue forces, national disaster medical system teams, pharmaceutical stockpiles and the national stockpile cache.
- The US Coast Guard, which deployed boat crews, law enforcement border teams, pilots, support personnel and helicopters for interdiction and surveillance.
- US Customs Border Protection, which was responsible for smoothly processing over 700 international attendees, as well as X-ray equipment to scan commercial vehicles.
- The Transportation Security Agency (TSA), which deployed screeners and security inspectors.

A number of criteria are taken into account in deciding which events are to be called NSSEs. Most prominently, these include the number of expected attendees and participants, the social and symbolic importance and heavy attendance by domestic and foreign dignitaries. Over the past four years, 20 events have been officially designated NSSEs. These included the presidential inaugurals of 2001 and 2005, the 2002 Winter Olympics, both the Republican and Democratic conventions of 2004, last year's G8 summit, the annual Super Bowl and the memorial service for Ronald Reagan.

THE EVOLUTION

As described by Mazur, NSSE security practice is a constantly evolving area combining classic procedures used by the Secret Service and law enforcement for decades with new areas of expertise.

"In many ways," he said, "the basics of securing highly sensitive events haven't changed. The classic repertoire of event security, including fencing in areas, maintaining barricades, special access badges, sharpshooters, rooftop surveillance and K-9 teams, remains important. One shift,

though, especially since 9/11, is that there's been a dramatically heightened awareness of the need to more effectively deploy new technologies."

This shift is opening up an important new venue for information technology companies offering a diverse mix of devices, including wireless communication systems, video surveillance, weapons detectors, environmental monitors and night vision equipment.

WIRELESS NETWORKS

A basic and daunting challenge in mounting special events security is putting together a viable communications infrastructure, often in adverse circumstances and always in a hurry.

"It used to be all that law enforcement and safety officials covering an event needed were police frequency walkie-talkies," recalled Mazur. "But in an era when just about everyone at a big event has a cell phone—and even a cell camera—that's not nearly enough."

At the presidential inauguration ceremonies last January, an alert visitor may have noticed, in addition to all the pomp and circumstance, numerous white vans and trailers scattered across the National Mall, each with 40-foot-high microwave dishes, antennas and racks of radio gear. What they were seeing was the rapid deployment of mobile cellular towers to support the needs of what was effectively a temporary city within a city.

"They say Rome wasn't built in a day, but the challenge of putting up a wireless voice-data communications infrastructure for an NSSE really is like building a city overnight," said Greg Meacham, vice president of Homeland Security Services of Virginia-based Nextel Communications, a major provider of cellular networks to the Secret Service, FBI and other federal and local law enforcement agencies.

Nextel has been a regular provider of wireless voice and data at NSSEs, including, in addition to the inaugural, the G8 summit, Reagan funeral services and Republican and Democratic conventions. At each event, it was charged with the responsibility of putting together a customized network with little lead-time.

Preparation for the January 2005 inaugural entailed more than doubling the cellular capacity of downtown Washington, DC.

"The problem," Meacham said, "wasn't that existing cell networks in Washington were deficient for normal use. They actually have fine coverage. But in a situation where hundreds of thousands of people would be using their phones simultaneously, the challenge of ensuring military and law enforcement communications is daunting."

To make communications at the inaugural come off without a hitch, Nextel deployed seven mobile cell towers, known as cell on wheels (COWs), in a 1-mile radius around

JIM YOUNG/REUTERS

Preparations for potential biological or chemical incidents are an essential part of National Special Security Event measures. Above, Inspector David Tyndall of the Denver, Colo., hazardous materials team is helped into his protective suit by Rex Cross, the weapons of mass destruction coordinator, during the G8 summit.

the Capitol. They also added more than 100 radios to rooftops along the parade routes. In only one month's time, between mid-December and Jan. 20, the company added as much network capacity to downtown Washington, DC, as it normally would in three years in a typical urban neighborhood of similar size.

If ramping up communications in an urban area is tough, NSSEs in other areas have challenges all their own.

"You'd think with a situation like the G8 summit, where we had many months of lead-time, it'd be a little easier, but there are always strange twists and turns," Meacham said, recounting two unforeseen problems in setting up wireless data networks for the summit, which was held on an island off the coast of Georgia. "One important agency had received a building well in advance, and we'd made sure that [the agency] had an infrastructure in place," he recalled. "But suddenly—literally at the last minute—their center of operations had to be changed due to demonstrations taking place. They got shuttled to the garage bay of an all-concrete building with no signal reception at all. We had to have an emergency team come in, and they had only a few hours to put something in place. It wasn't pretty with all the tie-wraps and cables on the floor, but they got it done.

"In another part of the summit area," he added, "five government agencies had rented a religious retreat. When we got there, we realized they hadn't done a full RF [radio frequency] survey on many sections of the property. For instance, the soccer field where they had planned to take off and land helicopters had no communications service. To add to the dilemma, by the time they moved in, security was already fully locked down. Our cell on wheels emergency team had made it through various layers of perimeter security, where it was stopped and questioned numerous times."

SURVEILLANCE AND DETECTION

Maintaining effective video surveillance at a special event also entails a more flexible, mobile approach to technology.

At the January 2005 inaugural, UK-based Orthogon Systems provided secure, high-bandwidth connectivity between security cameras along Pennsylvania Avenue and a security command center in Herndon, Va. The wireless system, called OS Gemini, was designed to connect video feeds across obstructed non-line-of-sight paths with high levels of interference.

As Rob Franklin, chief operating officer of Virginia-based Morgan Franklin, a leading IT consultant and systems integrator for the federal government, recalled:

"At the inaugural, law enforcement had to deal with a dense urban environment and an unusually high level of both signal interference and physical obstacles preventing or interrupting non-line-of-sight connections. OS Gemini allowed us to locate the security cameras where they were most needed, regardless of obstruction and noise, enabling real-time surveillance throughout the ceremony."

The Ethernet bridge system provided 33.6 mega-bit-per-second (mbps) broadband connectivity throughout high-interference zones. Each end of the OS Gemini link consisted of an integrated outdoor unit and a small powered indoor unit, and included an embedded web server. Each unit employed wide-beam antennas that were aligned using an audible signal strength that translated the received signal strength into an audio tone.

"To be effective in a special event situation," said Orthogon CEO Phil Bolt, "you need to develop special skill sets. Specifically, you have to be willing to improvise in an environment where there is a lot of uncertainty and variability. You often have places where there's no infrastructure or just a rudimentary infrastructure inadequate to what good security requires. You have to get creative about finding ways to get power and capacity to the right places at the right time. In an urban environment, you have buildings, trees, monuments and other fixed objects that can interrupt your standard systems. And another concern, one we were very concerned with at the inaugural, was large moving obstacles. Imagine terrorists using a large truck to block video surveillance from a crucial location to the command center."

At the Republican National Convention in New York last summer the New York-New Jersey Port Authority's tactical team, the Emergency Services Unit (ESU), was called on to secure the many bridges and waterways that lead into and surround Manhattan Island.

The waterways are not well lit, and maintaining effective nighttime surveillance required the ESU to use night-vision tools—originally designed for the US military—from White Plains, NY-based ITT NightVision.

ITT's PVS-14 goggles work using what's called Generation 3 image intensification technology. The goggles take the small amount of light that's in the surrounding area (for example, starlight) and converts the captured pho-

tons into electrical energy or electrons through an image identifier called a pinnacle tube. These electrons in turn pass through a microchannel plate containing 6 million channels. As electrons strike channel walls, they multiply and are projected onto a phosphor screen, which enlarges, brightens and intensifies their image.

"The tube allows law enforcement the flexibility of moving between different lighting conditions while maintaining a clear image through the goggles," explained ITT spokesperson Courtney Reynolds. "With the pinnacle tube and its gated power supply, officers can move easily from low light to lighted conditions as the unit automatically adjusts the image based on the level of illumination. This allows officers to move from very poorly lit waterways and port areas into urban areas that are better lit but still require image intensification."

At future NSSEs, ITT NightVision hopes to provide an enhanced version of the current goggles based on sensor fusion, the optical overlay of imagery from an image intensification sensor with imagery from a thermal sensor. "This advance," Reynolds predicted, "will allow users to see through fog, smoke and other obscurants. For the even longer-term, we're working on a digital unit that will connect image intensification and thermal imagery to a digital output and electronically fuse the two images pixel by pixel."

And visual systems are not the only forms of detection employed at NSSEs. At the most recent Super Bowl, Sunnyvale, Calif.-based RAE Systems was called upon to deploy an ad-hoc multisensor chemical and radiation detection network, using its proprietary Area RAE units. The units contain data radios that enable real-time data transmission with a base controller located up to 2 miles away. The device uses a highly sensitive photo-ionization detector for parts-per-million measurements of volatile organic compounds, and up to two electrochemical toxic sensors for measurement of specific toxic substances such as carbon monoxide and hydrogen sulfide.

IT AND DATA

Once communications networks and information gathering surveillance technologies are in place, an additional challenge is deploying tools that allow the barrage of relevant and irrelevant data coming in from the field to be assimilated by command centers.

During the G8 summit, public-health officials throughout the state of Georgia successfully deployed Stout Solutions' "First Watch " technology to notify them any time a suspicious package, powder, bomb threat or explosion was reported anywhere in the state's 911 system. Analytic software developed by Stout allowed the emergency medical command center set up in Savannah, Ga., for the summit to identify and track any pattern or syndrome suggestive of a bio-terror attack or other public health danger. The system aggregated data not only from 911 but from emergency medical computer-aided dispatch. A software program called ProQA enabled responders in the affected jurisdictions to identify threats or dangerous trends based on predefined criteria.

At the inauguration, five crisis management and collaboration software systems developed by E Team, based in Los Angeles, Calif., helped manage law enforcement activities and facilitate information coordination between the Washington, DC, police department, the George Washington University Medical Center, the US Department of Health and Human Services, the Center for Disease Control and Prevention and the Strategic National Stockpile. The software enabled security information to be culled from over 6,000 state, federal and local law enforcement officers on the ground, on rooftops and in the air throughout the city.

Special event security is no different from day-to-day security as practiced in more permanent locales. In fact, it represents all the fundamentals of every day security raised to a higher level of intensity.

While information management tools such as these shine brightest in a crisis or in high-profile situations like an NSSE, they frequently remain in place after the special events are over, and become integrated into everyday security use. After the G8, for instance, a medical alert system was kept on for full-time use in the Georgia public health system.

"The challenge every technology vendor who works with special events faces is to come up with products that can be adapted for one-time, one-of-a-kind situations, but can also be sold for more general purpose use, once the big event ends," Stout reflected.

ANALYSIS

Special event security is no different from day-to-day security as practiced in more permanent locales. In fact, it represents all the fundamentals of every day security raised to a higher level of intensity.

Because each special event is unique, everyone involved in an NSSE needs to cultivate every skill and utilize every tool possible to increase speed and flexibility of response and adaptability to ever-changing environments and situations.

As Tom Mazur put it, "We can provide working blueprints for how the division of labor and flow of information should work in theory, but in the most basic way, every special event by definition is special—that is, unique. So special event teams need to reinvent their strategy, operations and tactics for each event and its challenges."

In facing these challenges, technology is not an end in itself—but it is an increasingly useful and necessary tool. HST