Dr. Fred Roberts
Professor of Mathematics at Rutgers University and Director of the CCICADA Center
Mass Gathering Security: A Look at the Coordinated Approach to Super Bowl XLVIII in Newark, New Jersey and Other Large Scale Events
June 23, 2014

My name is Fred Roberts. I am a Professor of Mathematics at Rutgers University in Piscataway, NJ and I am Director of the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA). CCICADA was founded as a Department of Homeland Security University Center of Excellence, is based at Rutgers, and has 16 partner institutions across the US. It is part of the network of Centers of Excellence created by the DHS Office of University Programs. CCICADA's work is based on data analysis and we work on modeling, simulation, and decision support. We work with many federal, state, regional and local government agencies and with the private sector.

DHS has been a strong supporter of CCICADA's work on stadium security. Through the DHS university programs support, we feel that we have developed a real expertise in this area, one we could never have developed without DHS University programs. This work commenced in 2010 when we worked on simulation of stadium evacuation in collaboration with one of our private sector partners, Regal Decision Systems. Regal's evacuation tool helped half a dozen stadiums plan evacuations and was instrumental in allowing MetLife Stadium in New Jersey to evacuate safely during a preseason game in its first year of operation when there was a lightning storm.

Work on stadium evacuation has led us to collaborate with all major sports leagues, as well as college and minor league sports, and also to study safety and security at malls, bus and rail terminals, amusement parks, and other places where people gather. These gathering places are attractive targets for terrorists and criminals, and increasingly more so as such iconic targets as the Pentagon and the Capitol are "hardened."

Based on our early work on stadium evacuation, we began to collaborate with stadiums on patron screening procedures and eventually developed a tool that enables stadiums to determine which types of inspection (wanding, pat-downs, bag inspections, walk through magnetometers) will work best in their environment, taking into account the number of patrons expected, the weather conditions, the amount of time each type of inspection takes, etc. Because of the initial success of this tool, I was asked to present it to the National Football League's security seminar last week, a meeting attended by security directors of stadiums and venues all across the NFL.

We have also worked on models of crowd management and on prevention of human trafficking at major sports events such as the Super Bowl.

In 2012, CCICADA was asked by the DHS Office of SAFETY Act Implementation to develop a "Best Practices Manual" for stadium security from a counter-terrorism point of view. This manual, delivered in July 2013, was meant for OSAI to use as a tool to evaluate applications from stadiums for SAFETY Act designation or certification, and for stadiums to use as a tool

in preparing their applications. As part of the process of developing that manual, we did an extensive literature review and held interviews with and visited venues from all major sports leagues, as well as college and minor leagues. We also held a workshop on stadium security at Rutgers in 2013. We are now working on additional aspects of stadium security for OSAI, expanding on our earlier work, to develop metrics, measures of effectiveness, and good ways to test for training. OSAI would also like us to work on the economics of stadium security and on the use of randomization in screening, credentialing, and other aspects of stadium security.

Our work has led us to some observations that were a surprise not only to us but to a number of the security experts we interacted with. Here are a few examples.

Increasingly, physical systems are run by cyber systems. In our modern stadiums, this is true of heating and air conditioning, message boards (including for emergency messages), access control within the facility, escalators and elevators. But these systems can fail due to deliberate action of others. Thus, cyber security in our nation's stadiums is a major concern. At Super Bowl 47 in New Orleans, the lights suddenly went out. My first reaction was that this was a cyber attack. Fortunately I was wrong. However, it was a warning sign.

While a great deal of attention has been paid to hardening access to a stadium, the exterior of the stadium becomes a softer target. Today's modern automobile is a good example of a collection of physical systems that are increasingly run by cyber systems. Modern cars are already semi-autonomous and there is work being done on totally driverless cars. We have already seen that it is possible to hack into a modern car and control its braking, acceleration, steering, etc. What would happen if someone hacked into a car in the busy parking lot when thousands of people are packed together tailgating?

There is a great deal of consensus that walk through magnetometers are more effective in detecting dangerous materials than other screening systems such as wanding or pat-down. Yet, there are issues that need to be resolved about magnetometers. Early evidence seems to be that they might not work so well in bad weather, especially wind. Also, so that they don't block the way in case of the need to evacuate, at least one stadium has experimented with putting them on wheels. But does this affect their accuracy? Magnetometers also involve a major capital expense for a venue and because they require much more space than wanding or pat-down, might even require a stadium to give up some of its parking lot to make room for them. What incentives are there for management to do this?

Food security is an issue addressed with widely varying degrees of effectiveness and thoroughness at our nation's stadiums. Effective measures can be as simple as putting out condiments in packets, rather than large dispensers that make targets of opportunity for chemical or biological agents. However, not all stadiums are well versed in food security.

Information about the physical facilities at a stadium is often available to the public, e.g., when new building plans are filed. This could be a serious vulnerability.

Background checks for employees are a key component of a stadium security plan. But it is very difficult to find out about changes in background after an employee has been hired. How does one find out about new problems with the law, for example? Could repeat of background checks be required? They are expensive, and one possible model might be to perform them randomly from time to time.

Domestic violence/workplace violence are issues for stadiums. Disgruntled spouses and others can be a problem. Does the stadium obtain information about restraining orders that employees are served? Should it be easier to obtain such information than it is now?

Do employees receive a copy of an emergency plan? Are they required to return it when they leave employment? Do they receive it electronically and, if so, how can we be sure they do not make and/or maintain a copy?

As I said, our work has taken us to all kinds of venues. Several, such as Yankee Stadium, MetLife Stadium, Citi Field, have already received SAFETY act designation or certification. Achieving such status reflects the professionalism and extensive emphasis on security at these venues. However, less well off owners of venues and sports franchises do not have the resources to invest in security in the way that these large and highly successful examples do, and this is even more the case for minor league venues. Just as "hardening" of the Pentagon and US Capitol and other iconic targets can direct the attention of terrorists to iconic sports stadiums, hardening of those stadiums can direct the attention of terrorists to sports venues that are less secure. If the object is to disrupt the enjoyment of our gathering places, and create terror, an attack at a minor league venue could have a significant impact.

The events at the Boston Marathon demonstrate the difficulty of protecting large crowds that gather for events where there is no natural access control. Last week our students and faculty were official security observers at the USA Special Olympics in New Jersey, where some of the venues had similar issues of access control, and we will be helping the Special Olympics management write an After Action Report that will inform the next organizers of this important event. We have already learned from the Boston Marathon to take measures at our stadiums where access control is possible to set up perimeters so as to minimize the possibility that screening procedures themselves will create vulnerabilities by creating long lines of people in a small space. However, Boston-type vulnerabilities exist in the areas outside the stadium screening areas.

It is not possible to protect people in large gathering places from all hazards, especially in an open society such as ours. However, with appropriate research, with true partnerships among government, the private sector, and even those of us in academics, the risk can hopefully be reduced.