Detecting Concealed Weapons: Directions for the Future

by Chris Tillery

About the Author

Mr. Tillery is the associate deputy director for science and technology at the National Institute of Justice.

On July 24, 1998, a man entered the U.S. Capitol building in Washington, DC, with a .38-caliber handgun concealed under his clothing. A security check point with a portal weapons-detection system had been established at the entrance of the building. Knowing that his gun would be detected if he walked through the portal, the man stepped around it. Immediately, he was confronted by Jacob Chestnut, one of the Capitol Police officers operating the portal. The man drew his gun and killed Chestnut. He then shot and killed a second officer, John Gibson, before he was stopped.[1]

Seven years later, on December 5, 2005, a man with a bomb vest under his clothing approached a shopping mall in Netanya, Israel. His behavior alerted police and mall security. When he was confronted outside the mall, the suicide bomber detonated his bomb, killing 5 people and injuring 50.[2]

Although there has yet to be a suicide bombing in this country, such an attack could happen anywhere—on a bus, at a mall, at the Super Bowl, or at the Academy Awards. It is vital for law enforcement to be able to detect and respond to weapons at a sufficient distance to allow officers to make decisions and take actions that deal safely with the situation. For over a decade, the National Institute of Justice (NIJ) has been working to address this need.

Limitations of Current Weapons-Detection Systems

The incident at the U.S. Capitol showed the limitations of current security-detection portal systems—they must be near an individual to work. They generally provide sufficient warning when it comes to detecting a knife, but they cannot detect weapons that can kill beyond arm's reach. By the time a handgun or a bomb vest is detected, it generally is too close to be dealt with safely.

But there are ways to provide more warning. One is to move the portal farther from the operator. For example, it can be incorporated into a building's entrance and operated from a control room at another location. A person who wants to enter the building is then required to first go through the portal before an interior door opens to allow admittance to the building. If the portal detects a weapon, the operator does not open the interior door or the door locks automatically, without the operator's intervention. To further protect the public, exterior doors open only after a second interior door is closed behind the person who has entered. In this way, only one person at a time can enter the building, preventing the possibility that innocent bystanders would be trapped in an entryway with an armed person.

Despite their advantages, remote portal weapons-detection systems have significant limitations. They require more space for the remote location, which is not always available, and they impede traffic flow. Using a remote exterior door with screening equipment and a second interior door in a crowded venue, such as a sporting event or an airport, would impede the flow of pedestrian traffic and cause people to collect in a relatively small area, creating a prime target for a suicide bombing or other attack.

Another approach to detecting concealed weapons is through the use of back-scatter x-ray weapons-detection systems, which use low-dose x-rays to develop images of objects under clothing. The x-rays pass through clothing and are reflected—or "scattered back"—by the skin. These systems have the same limitation as existing portal weapons-detection systems: They require close proximity to detect a weapon. They can, however, reduce the nuisance alarms that occur when metal objects other than weapons are detected and thus move pedestrian traffic more quickly through security checkpoints.

Where Are We Going?

In the late 1990s, NIJ launched an aggressive program to find ways to detect concealed weapons from a safe distance. The Institute investigated a wide range of potential solutions—radar, infrared radiation cameras, acoustic devices—and determined that passive millimeter wave (MMW) cameras offered the greatest potential.

Use-of-force protocols for dealing with an armed gunman, who may or may not be suicidal, may not be appropriate for dealing with a suicide bomber, whose device might be detonated remotely by an accomplice or by the bomber himself even after being restrained.

A passive MMW camera is one that does not use an artificial source of MMW radiation. It develops images from ambient MMW radiation, which, like infrared radiation, is all around but cannot be seen by the human eye. Although both infrared and MMW radiation can penetrate clothing to develop images of hidden objects, MMW radiation is more effective in this respect. For example, an MMW camera can develop an image through a heavy coat, but an infrared camera cannot.

Over the past decade, NIJ has leveraged research and development on MMW technology performed by the U.S. Department of Defense to the point that there now are commercially available MMW weapons-detection cameras.[3] These cameras represent a 10-fold decrease in size and cost from the initial prototypes, but much work remains to be done in improving resolution and range, and reducing weight and cost.

NIJ continues to work on developing the potential for MMW technology to detect concealed weapons. For example, the Institute is exploring the use of automobile collision-avoidance MMW radar; and in another project, it is supporting efforts to develop smaller, less expensive MMW cameras. NIJ is also reexamining other technologies, such as infrared cameras, that have advanced in the last decade and could offer new opportunities for the detection of concealed weapons.

New Technologies Demand New Protocols

New technology is never, in itself, the solution. Rather, the solution lies in adopting effective policies and practices for use of the technology. Emerging weapons-detection technologies pose complex questions for law enforcement agencies, particularly the development of legally defensible protocols for using them.

For instance, using a device to remotely search people walking in a public venue, without their knowledge, raises fundamental Fourth Amendment concerns with respect to lawful searches. When and under what circumstances can such a device be used? What is the public's reasonable expectation of privacy in a public venue? What constitutes probable cause for the use of these devices? What is a reasonable search?

Another issue is appropriate use-of-force protocols. The use of deadly force is governed by the totality of the situation. There are two salient points to keep in mind when developing protocols under these circumstances. The first is that no technology is perfect. An MMW camera may reveal an object that, in all likelihood, is a bomb vest, but there is still a possibility, however slim, that it may not be a bomb vest. The second point is that a suicide bomber, by definition, intends to kill or injure as many people as possible. Use-of-force protocols for dealing with a person armed with a handgun, who may or may not be suicidal, may not be appropriate for dealing with a suicide bomber, whose device might be detonated remotely by an accomplice or by the bomber himself even after being restrained.

Under the Nation's federalist system of government, the development of specific protocols for the effective use of these technologies must be done jurisdiction by jurisdiction. Jurisdictions need not work in a vacuum, however. Key professional public safety organizations have begun to develop guidelines, including ways for responding to suicide bombers. The International Association of Chiefs of Police (IACP), for example, includes this issue in its *Training Key* monographs, which provide officers with authoritative information on a broad variety of law enforcement practices and procedures. For more information on the IACP *Training Key* monographs, see www.iacp.org.

A New Century of Challenges

The new century brings with it new challenges in detecting concealed weapons. As criminal justice professionals work on the technology and protocols to address these challenges, NIJ will continue to provide the research and development that the Federal, State, and local law enforcement communities need to help prevent attacks and ensure the safety of citizens.

NCJ 219608

Notes

1. "Shooting at the Capitol, Special Report: From the Shootings to the Investigation," *Washington Post,* available at www.washingtonpost.com.
2. Myre, G. "Bomber Kills 5 Outside Shopping Mall in Israel," *New York Times,* December 5, 2005, available at www.nytimes.com.
3. Two commercially available products resulting from NIJ's investment in concealed-weapons detection are the Sago ST 150 (www.trexenterprises.com/Subsidiaries/sago.html) and the Brijot BIS-WDS (www.brijot.com). These products and manufacturers are cited for informational purposes only and do not constitute product approval or endorsement by the National Institute of Justice.

Recently Released by NIJ

Addressing Shortfalls in Forensic Science Education
May 2007

Many crime laboratories find that new graduates of forensic science education programs are not properly trained. This *NIJ InShort* explains the benefits of accredited programs. An accredited curriculum gives employers—such as crime lab directors—standard criteria to assess whether an applicant is qualified. This publication is available at www.ncjrs.gov/pdffiles1/nij/216886.pdf.

Mental Health Screens for Corrections
May 2007

This *Research for Practice* reports on two projects that created and validated mental health screening instruments, which corrections staff can use during intake. Short questionnaires help identify inmates who require mental health assistance. One screening instrument was found to be effective for men and is being adapted for women. The other has effective versions for both men and women. This publication is available at www.ncjrs.gov/pdffiles1/nij/216152.pdf.

Public Safety Communications and Interoperability
May 2007

Public safety agencies often have difficulty communicating with each other due to incompatible frequencies and equipment and lack of a common language. This *NIJ InShort* describes these barriers and offers recommendations to help overcome them. This publication is available at www.ncjrs.gov/pdffiles1/nij/214331.pdf.

Understanding FCC Narrowbanding Requirements
May 2007

The Federal Communications Commission has required all non-Federal public safety licensees currently using 25-kHz radio systems to migrate to narrowband 12.5-kHz channels by January 1, 2013. This *NIJ InShort* explains how those who do not meet the deadline may lose communication capabilities and provides guidance on how to prepare for the migration. This publication is available at www.ncjrs.gov/pdffiles1/nij/217865.pdf.

Voice over Internet Protocol
May 2007

Voice over Internet Protocol (VoIP) is a technology for encoding and routing digitized voice and data traffic over the Internet. This *NIJ InShort* discusses the technology's potential benefits and explores two types of VoIP particularly relevant to public safety. It also reviews issues to consider before implementation and introduces an emerging public safety standard that may allow interoperability between technologies. This publication is available at www.ncjrs.gov/pdffiles1/nij/217864.pdf.