Imaging, Speech Technology Boost Simulation Training

As the officer who just finished his training leaves the simulator, he whispers to his coworker: “Watch out for the big blond guy.” However, when the second officer starts the training scenario, there is no big blond guy to be seen. Their department’s Use of Force Training Simulator uses computer-generated images (CGI) instead of standard video scenarios, and the instructor has changed the “big blond guy” into someone small, slight, and dark-haired.

“You can use the basic scenario skeleton to change clothes, props, race, gender, and more,” says Tyson Griffin of the Naval Air Warfare Center Training Systems Division (NAWCTSD), the Office of Justice Programs’ National Institute of Justice’s (NIJ’s) partner in the creation of the Use of Force Training Simulator.

The simulator is expected to reach the prototype stage (prior to commercialization) by September 2008. By using CGI instead of videotaping performances by actors, the system can incorporate an array of features regarding character ethnicity, voice, gender, mood, and compliance, in addition to weather and time of day. These selections can either be generated at random or selected by an instructor, and an individual trainee’s voice and actions can greatly influence the ultimate outcome. Also, because the trainee’s visual system is built in a three-dimensional virtual space, the after-action review of an individual’s training can be more in-depth, allowing the instructor to use the mouse to pan and scroll around and replay the scenario in three dimensions rather than be limited by the fixed field of view shot by the camera during filming.

Even more influential than the variability introduced by using CGI is the speech recognition capability built into the system.

“The officer can have a conversation with the CGI characters. An individual can be very commanding or can totally fail to control a situation through speech,” Griffin says. “An officer can talk the suspect down and have a successful closing to the scenario without ever pulling a gun or using less-lethal weapons—or a situation could blow up sky high. This is a key concept to establishing a cognitive-based approach to training as opposed to a shoot/don’t shoot approach.”

Affordability also played a key role in the system’s design, because NIJ wanted to produce a system that smaller law enforcement agencies could afford. The agency allocated development dollars and NAWCTSD provided development expertise. When the prototype becomes available as a commercialization opportunity in September 2008, the ultimate cost to law enforcement agencies should comprise only the cost of the materials needed to build the system, a reasonable profit by the chosen vendor, and the cost to develop any new scenarios, Griffin says.
the Office of Justice Programs’ National Institute of Justice, is developing the Correctional Operations Trend Analysis System (COTAS), an automated way of predicting inmate disruption and helping administrators find ways to minimize it.

Once COTAS is operational, sometime in 2009, Florida plans to share the concept, the codes, and the processes it used to develop COTAS with other correctional facilities. Other systems can then adapt COTAS to their own methods of gathering data and technology requirements.

“The potential that COTAS offers to correctional administrators at the institutional, regional, and State levels is tremendous,” says James Upchurch, Chief of the Florida Bureau of Security Operations. “There are other States that have systems in place where they automate data and information to managers in a user-friendly form, but the primary difference with COTAS is its predictor capability that allows managers to do something ahead of time.”

The Florida Department of Corrections, the third largest State correctional system in the Nation, presently houses 96,000 inmates and has more than 150,000 offenders on community supervision. The system comprises 135 facilities, 60 of them major, and employs 25,000 individuals, including 17,000 uniformed officers and supervisors. Obviously, a system of that size generates a staggering amount of data; in addition, Florida maintains records back to the 1970s.

That’s the point from which the research and data analysis team, headed by David Ensley, Dena French, and Kristine Dougherty, began. They worked through a lengthy analysis process that resulted in the identification of the major predictive indicators now programmed into COTAS. (Indicator examples include drug-testing percentages from the random-drug testing program, inmates’ mental health history, and housing classification scores.) The team conducted statistical analyses of years of data on violent and nonviolent disruptive events at the individual and facility level.

The information technology team, headed by Tommy Tucker and Frank Wood, took these predictors and created a user-friendly interface (now in the beta testing phase) with dashboard/gauge presentation of critical elements and the capability to drill down through additional layers of data detail. The gauges compare the situation in any given institution to other similar facilities throughout the State. The development process also included automating a daily feed of data into the COTAS system.

Beta testing began on a small scale in April and will slowly expand during the remainder of 2008, with users providing feedback for modifications to be implemented before final rollout next year.

“We wanted to create a user-friendly system that would eliminate the need to spend hours of time reviewing mountains of reports, and make a way to monitor the ‘health’ of the various institutions accessible from the warden level to the secretary level,” Upchurch says. “We hope this will take us from being reactive to being more proactive.”

For more information, contact James Upchurch, Chief, Bureau of Security Operations, Florida Department of Corrections, at 850-410-4390 or e-mail upchurch.james@mail.dc.state.fl.us.
episode. Along with creating these additional scenarios, developers are working on documenting the process of authoring scenarios so that in the future, law enforcement agencies could potentially produce their own role-play scenarios.

In the meantime, the team at NAWCTSD is working on refining the existing scenarios, some of which include up to 100 different “branches,” depending on how a trainee reacts.

“Characters can have four moods, ranging from compliant to defiant,” says Simmonds. “There are also preassault indicators such as kicking a can, clenching a fist, and raising a voice when speaking.”

Griffin and Simmonds caution that only the largest agencies may be able to invest the time in training personnel to create scenarios, as some programming knowledge will be needed. NAWCTSD staff, however, hope to incorporate a basic artificial intelligence capability (a list of actions and responses) into the CGI characters to assist agencies in the creation of their own exercises. Also, NAWCTSD and NIJ are discussing the establishment of a central repository for all scenarios created by training system users that would be freely accessible to all law enforcement agencies that have the system.

Other refinements planned for inclusion in the commercialization prototype call for further miniaturization of the weapon module technology that would allow officers to use their own weapon and duty holster combination, and the introduction of other less-than-lethal options such as “pepper spray” in addition to service weapons and other less-lethal weapons. Even without any further refinements, the existing system can be set up and taken down in less than an hour, in a space no greater than 20 feet by 20 feet in dimension.

“It’s very easy to set up and take down. It’s very portable, and very easy to use,” says Griffin.

For more information, contact Sunny Simmonds, 407–380–4699, asuncion.simmonds@navy.mil; or Tyson Griffin, 407–380–4671, tyson.griffin@navy.mil.
Making his best attempt to catch a fleeing suspect, a police officer rounds a corner into a dark alley, unsure of what lies ahead of him. The flash of a .357 revolver cuts through the darkness and he falls, shot in the chest, brought down by one of the many dangers officers face every day. However, because the officer had on his personal body armor, he got up and walked out with a bruised chest . . . and his life.

Since the International Association of Chiefs of Police (IACP)/DuPont™ Kevlar Survivors’ Club® was established in 1987, more than 3,000 individuals working in law enforcement have survived both ballistic and nonballistic incidents because they were wearing body armor. Of the approximately 1,200 officers killed in the line of duty since 1980, more than 30 percent might have been saved if they had worn vests.

A study conducted by the FBI in 1994 estimated that an officer not wearing body armor has a risk of dying from gunfire that is 14 times greater than for officers who do wear armor. In 2003, the Office of Justice Programs’ National Institute of Justice (NIJ) developed a pilot program to assess injuries caused by less-lethal devices in the field in near real time. In 2006, NIJ evaluated the usefulness of this framework for understanding injuries to officers wearing body armor, and subsequently decided to fund a pilot study focusing on blunt force trauma injuries (bruising, lacerations, and/or internal injuries caused by a bullet striking but not penetrating a vest).

Although final study results will not be available until 2009, some preliminary conclusions have been drawn:

- When an officer is shot in an area covered by body armor, resulting injuries will not always be obvious. Bringing the body armor to the hospital may help the emergency physician diagnose injuries. Even if no injury is apparent in the wake of a shooting, the officer should still seek medical attention because of the possibility of internal injuries.

- Accurate records about ballistic information (including caliber, grain, and barrel length), as well as the distance between the officer and shooter, are also key in assessing injuries. These records and other information such as how the vest fit at the time of the shooting, number of shots, and shot sequence should be collected within 15 minutes of the incident, or much of this information can be lost.

- Because of the infrequency of officer shootings in most communities, formal guidelines to help emergency room physicians diagnose or treat blunt trauma injuries do not exist. An international panel of experts that is analyzing results of the study is compiling draft guidelines to address this and exploring ways to distribute this information to hospital emergency rooms.

- A tag on the vest that leads to a website that provides the latest information on medical treatment for blunt trauma injuries could prove a great asset to the medical community, as could an Internet resource on how to collect information on the event for later analysis.

- A recommendation that after an event, even if there is limited visible bruising, the officer seek medical attention in case forces were propagated into the body.

- Events of this type also cause psychological trauma and may require long recovery times. Also, the incident’s effects may extend beyond the workplace to include the officer’s family.

The international panel of experts that is performing the review and analyzing incidents is cochaired by Dr. Cynthia Bir of Wayne State University and Joe Cecconi of NIJ. The Survivors’ Club collaborated with Wayne State University to determine the types of injuries likely to occur. Emphasizing injuries sustained and possible long-term health effects, the panel is reviewing actual field data to determine what injuries occurred, estimate their severity, and analyze whether injuries are being fully assessed. The 65 participants, who agreed to release their medical records and contact information for the purposes of an interview, were drawn on a volunteer basis from members of the Survivors’ Club.

The panel is reviewing, discussing, and analyzing each participating case, and generating input on injuries sustained and ways to improve the care the officers received. The panel will also examine better ways of collecting data. Surviving officers participate in discussions and recount their own personal experiences, giving the panel a broader understanding of the incidents, the overall care received, and the recovery process.

The panel will continue its work throughout 2009. The researchers want to thank the volunteers who participated and are looking for more volunteers who are still interested in having their cases reviewed.

For more information, or to volunteer to participate, contact Joe Cecconi, senior scientist, Office of Science and Technology, Operational Technologies Division, National Institute of Justice, at 202–305–7959, joseph.cecconi@usdoj.gov; or Cynthia Bir, Ph.D., associate professor, Wayne State University Biomedical Engineering, at 313–577–3830, cbr@wayne.edu.
A high school in Spokane, Washington, a student with a gun barricaded himself in one of the science classrooms on September 22, 2003. Using Rapid Responder®, a tool designed to coordinate response to emergencies, a safety officer at another school brought up a floor plan and photographs of the room, which provided crucial information to officers on the scene. Although the student ultimately received nonfatal wounds in a confrontation with SWAT team members, Rapid Responder helped responders safely defuse the situation with no further injuries to officers, students, or staff.

Following the Spokane incident, the Claremont (California) Police Department became interested in the software as a way to help officers in the field fill in blind spots when confronting dangerous situations in unfamiliar territory. In 2006, the department approached the National Law Enforcement and Corrections Technology Center (NLECTC)-West for assistance in funding the installation of Rapid Responder at Claremont High School as a technical pilot project. According to the Center’s Matt Begert, a year of meetings and discussion resulted in the installation of the software in August 2007, just before the start of a new school year. It had been in time for the Claremont Police Department to practice using the system in conjunction with their active shooter training.

In return for funding the project, we will be able to learn from their use of it over time, and figure out where there might be the possibility for improvements, Begert says. We’ll also be able to show it to other jurisdictions and agencies who might want to implement the software.”

Begert expects the observational phase of the project to last 1 to 2 years, with the end product a determination of how useful the software is to agencies and how the software will be shared with the product manufacturer.

Claremont began collecting information on the product’s use immediately with the August 2007 training.

“From that training, we realized what a valuable tool it was, and we currently have a grant application (U.S. Department of Education, Readiness and Emergency Management for Schools program) submitted to install it in all 12 public schools and 9 campuses in the school district,” says Claremont Capt. Gary Jenkins.

The active shooter training took place in a cordoned-off section of Claremont High, in a group of classrooms clustered around a small courtyard. Officers were divided into groups of four, instructed to move in a diamond formation (one officer leads, two officers assume flanking positions, and one brings up the rear), and sent through a battery of different scenarios. Before each contingent began a training session, its members received a briefing on the layout of the classroom and the courtyard and used the software tool. During the training, officers carefully maneuvered through the courtyard and classroom seeking two active shooters. In some scenarios, other officers pretending to be wounded students simulated panic and caused chaos as they ran through the courtyard. Shooters also used these pretend students as hostages.

“Before we had this, the officers essentially would tactically respond to situations without any specific knowledge about the area they were entering,” Jenkins says. “With the software, officers could review the setup of the area, including floor plans, doors connecting class rooms, and so on. It gave the officers the ability to employ better officer safety tactics, and was a huge advantage in planning how to operate as a team, how to move as a team, and even how to retreat if need be.”

Like many similar tools, Rapid Responder was developed in response to the 1999 Columbine High School tragedy. In the aftermath of that shooting, when it was pointed out that better communication might have provided a more effective response to such a crisis, several members of the Washington Association of Sheriffs and Police Chiefs (WASPC) began identifying ways that would help first responders communicate better in similar situations. Prepared Response, developer of the software, used that input as a starting point to create a sophisticated tool that first responders can use to coordinate their actions when responding to a variety of situations. During an actual event, all emergency responders have access to previously agreed on plans as well as access to the most up to date and reliable information about the environment. This increases the likelihood that all units responding to an emergency can work together.

The software helps agencies and jurisdictions coordinate the actions of emergency responders by collecting hundreds of pieces of information about a building and its environs and organizing these data points in a user-friendly display. Information that can be compiled in the system includes evacuation plans, floor plans, utility shutoffs, and photographs, giving first responders immediate access to critical information and enabling them to respond to crises quickly and efficiently. The software can be loaded on a laptop, made accessible via the Internet, or carried on CD-ROMs and flash drives. This means that on the road, even in a command post with out Internet access, emergency responders can access the tool.

“We wanted to be prepared if confronted with a situation like Columbine and the number of events that have occurred since then,” Jenkins says. “We wanted to make sure we had something at our disposal, and this one just seems to provide the information that would be critical to us in responding to that type of event or in a natural disaster such as an earthquake or wildfire.”

He explains that something as simple as knowing where the utility shutoffs are might make a difference in responding to an incident, and this software puts that kind of information at their fingertips. Claremont PD also knows who on the school staff has certain responsibilities, which would help the department better coordinate efforts with the school district.

It’s something that we hope we never have to use, but the way we look at it, we hope for the best, we prepare for the worst,” Jenkins says.

This product appears on the U.S. Department of Homeland Security’s Office for Domestic Preparedness Authorized Equipment List, which can be accessed through https://www.safetyact.gov/.

For more information on this project, contact NLECTC West, 888 548 1618 or Michael O’Shea, National Institute of Justice program manager, at michael.oshea@usdoj.gov or 202-365-7954.

Responders Knowledge Base

Agencies looking for information on products, standards, certifications, grants, and other equipment-related information might consider visiting the Responder Knowledge Base (RKB) website (www.rkb.us).

The site contains information on more than 5,000 technology products for first responders, and visitors can compare up to three products at a time. RKB also contains news releases and additional services available only to members.

RKB is funded through the Federal Emergency Management Agency National Preparedness Directorate, a division of the U.S. Department of Homeland Security (DHS). It features data items from other DHS-sponsored sites, such as the System Assessment and Validation for Emergency Responders (SAVER) site, the Lessons Learned Information Sharing (LLIS) system, and the ANSI Homeland Security Standards Database (HSSD).
BURGLARS GO BUST: The DNA Field Experiment

Between November 2005 and July 2007, the Office of Justice Programs’ National Institute of Justice (NIJ) provided funding to five communities (Los Angeles, Topeka, Denver, Phoenix, and California’s Orange County) to take part in a study of the effectiveness of DNA forensics in the investigation of property crimes.

Participating communities collected potential sources of biological evidence from up to 500 crime scenes between November 2005 and July 2007. Project protocol assigned half of each area’s cases to a control group, while biological material from the others underwent DNA testing. The majority of crime scenes sampled were residential burglaries, with the remainder coming from commercial burglaries and automobile thefts.

A detailed report on study results, The DNA Field Experiment Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes, can be downloaded from www.ojp.usdoj.gov/nij/topics/forensics/dna/property-crime/welcome.htm. Key results are summarized below. See sidebars for highlights of study outcomes in three participating cities (Denver, Los Angeles, and Phoenix).

Key study results:
• Cases with DNA evidence yielded twice as many suspects identified and arrested, and more than twice as many cases accepted for prosecution. Departments obtained suspect identification via Combined DNA Index System (CODIS) hits at twice the rate generated by the FBI’s Automated Fingerprint Identification System (AFIS).
• Additional costs incurred by departments averaged $4,515 per suspect identification and $14,178 per suspect arrest. Suspects identified with DNA evidence, however, had far more serious criminal histories. Thus, apprehension of these suspects seemed likely to have a disproportionate higher payoff in reducing the number of burglaries in a community, and potentially other types of serious crime as well.
• DNA samples collected by patrol officers seemed just as likely to yield good evidence than those collected by forensic technicians.
• Blood and saliva samples yielded significantly more usable CODIS profiles compared with cell samples obtained from items potentially touched by a suspect, such as a doorknob or a computer cable.
• Crime scenes where stolen property had been left unlocked yielded fewer good samples, as did crime scenes investigated between 2 p.m. and 10 p.m. (when departments often are at their busiest).

“We’d really like to get the message out to police departments around the country that there is a lot of information, some good lessons learned, in this report,” says Katherine Browning, NIJ program manager. The study used project data to complete its key goal of a cost-effectiveness analysis. Departments could find this information useful in requesting funding to expand their DNA programs to include property crimes.

“It’s best understood as a project that sought to test different approaches to the use of DNA as an investigative tool, and not as a test of established best practices, although Denver most closely followed established best practices and had the best outcomes,” Browning says.

Browning says NIJ is discussing the possibility of a 1-year followup project to examine convictions and outcomes.

What Is CODIS, Anyway?
Throughout this related group of articles are frequent references to the Combined DNA Index System, or CODIS. CODIS serves as an umbrella term describing all DNA index systems that match DNA profiles from crime scenes to a group of cataloged DNA profiles, some from individuals who have been identified by name, and others of whom, while not identified, have left DNA at the crime scene.

CODIS has three hierarchical components: national, State, and local. The national database is managed by the FBI under the authority of the DNA Act of 1994, and management of State and local databases varies by State. Each level has its own protocols and eligibility criteria; generally, criteria are stricter at the higher levels.

For more information, contact Katherine Browning, NIJ program manager, at 202–616–4786 or Katherine.browning@usdoj.gov.
Denver: Not in Our Town

It’s just another day on the job. Get up, have breakfast, grab a second cup of coffee, get in the car, drive to the job site. Make sure all the neighbors have left for work. Put on gloves, of course, and stroll to the unlocked window in the garage.

Another day, another break-in. Except this time, a beer can from the fridge that was left behind on the kitchen counter gets picked up by a law enforcement officer. No fingerprints, but there is saliva. Saliva that generates a CODIS hit. And suddenly, burglaries in this quiet residential neighborhood drop by an astonishing percentage.

During the 18-month timeframe of the DNA Field Experiment, the Denver Police Department arrested 95 individuals suspected of being prolific burglars, most of whom committed approximately 200 burglaries per year:

“They’re getting the message, don’t do it in Denver,” says Gregory LaBerge, director of the city’s Crime Laboratory Bureau, adding that Denver followed up its initial training push by returning to the city’s police stations and showing officers the effects of the program’s success.

“We’d ask, who collected that cigarette butt, and then tell the officer, ‘you got a hit, and after that, burglary in your neighborhood fell 40 percent,’” LaBerge says. “It showed them what was in it for them, and told them they did a good job. They really liked that. None of these officers had ever set foot in a crime lab, and initially they thought this was just another program. We showed them results, and now they think about DNA.”

The partnership with the district attorney’s office was essential because DNA matches were seen as useless without later prosecution.

The approach to officer training taken by the crime lab and the Denver District Attorney’s Office started with getting buy-in and participation from chiefs, commanders, sergeants, and other administrators, as well as the district attorney’s office, which agreed to file John Doe warrants on unidentified DNA to hold cases open. Officers received roll call training, repeated at 3-month intervals, and the city produced a DVD on identifying and collecting biological evidence and offered other training tips.

“In projects like this, you’ve got to include everybody,” LaBerge says. “We’ve used a team approach to everything in Denver for a long time. We didn’t just make the assumption that we knew how to train patrol officers; we sat down with commanders and got their input. We made sure they knew that burglary evidence might generate cross hits that would impact investigation of rapes and other violent crimes.”

“The approach to officer training taken by the crime lab and the Denver District Attorney’s Office started with getting buy-in and participation from chiefs, commanders, sergeants, and other administrators, as well as the district attorney’s office, which agreed to file John Doe warrants on unidentified DNA to hold cases open. Officers received roll call training, repeated at 3-month intervals, and the city produced a DVD on identifying and collecting biological evidence and offered other training tips.

“In projects like this, you’ve got to include everybody,” LaBerge says. “We’ve used a team approach to everything in Denver for a long time. We didn’t just make the assumption that we knew how to train patrol officers; we sat down with commanders and got their input. We made sure they knew that burglary evidence might generate cross hits that would impact investigation of rapes and other violent crimes.”

“Some people looked at this as a project, but we looked at this as a crime reduction strategy, part of a 5-year program,” he adds. “These projects can have an overall effect on crime in your city, not just on the targeted crime. Compared to other cities the same size, Denver’s overall crime rate took a huge drop.”

LaBerge says that using this decline as a selling point, the partners from the police department, crime lab, and prosecutor’s office were able to persuade the city to fund the new DNA policy on an ongoing basis, in spite of the city’s tight budget.

For more information on the Denver portion of the project, see chapter 4 in The DNA Field Experiment report, or contact Gregory LaBerge at 720-913-6561, email laberge@ ci.denver.co.us.

About the Benefits

Biological evidence collection? Laboratory testing? CODIS searches? Great tools to use in investigations of violent homicide and sexual assaults, where the likelihood of a perpetrator’s leaving DNA evidence behind is high and the magnitude of the crime is great. For burglary cases, maybe not so much. The processing expenses outweigh the benefits to society.

At least that’s the way some people thought before the DNA Field Experiment took place.

“It made a believer out of me,” says Commander Harlan Ward of the Los Angeles Police Department (LAPD), one of the key players in coordinating LAPD’s participation in the project.

“I was not particularly knowledgeable about the benefits of using DNA for solving property crimes,” he says. “I thought it was just something very expensive. Once I saw how many crimes were being solved and the type of suspects who were being arrested, I was convinced that this is the way to go in the future.”

The project coordinators in Los Angeles feel so strongly about the value of the processes developed during the DNA Field Experiment that they plan to approach the city council and the mayor to ask for funding to continue the project after the project report is published.

“Going into this, even I had certain prejudices about whether it would be worthwhile,” says Director Greg Matheson of the LAPD Criminalistics Laboratory. “When I started seeing the kind of people we were taking off the street, people with a long history of violent crime, I realized that even if we only pull these people off the street for 3 years on a burglary conviction, it’s a huge benefit to society. And if it’s a third strike, it could be 20 years or more.”

Ward cited the example of one suspect identified during the project who, at age 53, had 35 prior arrests and 23 prior convictions for a wide variety of offenses. “If you contract the expense of using DNA with the burden he’s placing on society, the benefits definitely outweigh the expense.”

This belief in the value of the project came after LAPD worked its way through an initial learning
A number of States around the country, including Colorado, have recently added a form of electronic messaging to their correctional facility mailrooms. Electronic messaging allows inmate families to write letters 24 hours a day, 7 days a week, and send them to their loved ones electronically for a small fee. The system’s features provide mailroom staff with the necessary tools to quickly scan letters, print out those that qualify, and quickly deliver them to inmates.

“Our mailroom staff have to open and read every piece of hard copy mail and check it for contraband,” says Tony Carochi, deputy director of prisons for Colorado. “Handwritten letters can be very difficult to read, and mailroom staff have to manually look for certain keywords or phrases. With electronic messaging, we put several hundred keywords that have been identified by Intel [Corporation] and security staff in a database, and the system reviews a letter in less than a minute. Using electronic messaging is a real timesaver.

Families and friends of an incarcerated person use the Internet to create an account, and purchase “e-stamps” to send their letters. The vendor’s interface system sorts and routes letters to the appropriate facility daily. Colorado had to purchase printers and copiers for printing the letters, but obtained the service at no cost.

Because not everyone has access to a computer, Colorado’s mailrooms still process a number of letters the “old-fashioned” way. The State introduced incoming electronic messaging in August 2006, and the next phase is for the introduction of kiosks that will allow inmates to send letters out through the system.

“We met with inmate advocacy groups before we introduced the pilot program and got their buy-in,” Carochi says. “We’ve had nothing but positive feedback from the advocacy groups, mailroom staff, inmates, and their families and friends.”

Colorado initiated this program as the result of an employee suggestion, and identified several vendors before selecting one for a four-month pilot program. The success of the pilot program led to the system’s statewide introduction.

For more information on Colorado’s messaging program, contact Tony Carochi at 719-426-4725, or tony.caroichi@doc.state.co.us.
TECHshorts is a sampling of the technology projects, programs, and initiatives being conducted by the Office of Justice Programs’ National Institute of Justice (NIJ) and the centers, specialty offices, and federal justice technology Centers of Excellence that constitute its National Law Enforcement and Corrections Technology Center (NLECTC) System. If you would like additional information concerning any of the following TECHshorts, please refer to the specific point-of-contact information that is included at the end of each entry.

In addition to TECHshorts, an online, biweekly technology news summary containing articles relating to technology developments in public safety that have appeared in newspapers, newsmagazines, and trade and professional journals is available through the NLECTC System’s website, JUSTNET, at www.justnet.org. This service, the Law Enforcement and Corrections Technology News Summary, also is available through an electronic e-mail list, JUSTNETNews. Every other week, subscribers to JUSTNETNews receive the news summary directly via e-mail. To subscribe to JUSTNETNews, e-mail your request to asknlectc@nlectc.org or call 800–248–2742.

Note: The mentioning of specific manufacturers or products in TECHshorts does not constitute the endorsement of the U.S. Department of Justice, NIJ, or the NLECTC System.

Public Awareness Campaign on Dangerous Video Games

**NLECTC–Northeast**

The New York State Division of Criminal Justice Services (DCJS) recently unveiled “Video Games and Children: Virtual Playground vs. Danger Zone,” a 20-minute presentation and accompanying video designed to help parents make informed decisions about the video games their children play to.

The presentation explores research on the topic of violent games, outlines risks, and provides parents with 10 tips to remember when purchasing games for their children. It also provides a primer on video game history and features video game content, ranging from “Pong” in the 1970s to the violent games being sold today. In addition, the video establishes guidelines for children’s play, including:

- Checking a game’s rating and reading the description, or renting a game, to preview it before purchase.
- Setting reasonable time limits and ensuring that children respect them.
- Discussing a game’s content and explaining why you object to certain games.

Staff from the NLECTC–Northeast Law Enforcement Analysis Facility provided state-of-the-art technology during the development of the presentation, including use of equipment that provided the tools needed to create a dynamic presentation. DCJS’ Missing and Exploited Children Clearinghouse created the 20-minute presentation, which is available at [http://www.criminaljustice.state.ny.us/missing/] and [http://virtualvideogame.htm](http://virtualvideogame.htm).

Rapid Gunshot Detection

**NLECTC–Southeast**

In March, NLECTC–Southeast conducted a test and evaluation of the ShotSpotter Rapid Deployment System (RDS) at the South Carolina Research Authority complex, the Center’s host agency. This recently developed wireless gunshot detection and location technology is part of Southeast’s continuing Wireless Gunshot Location Detection Project, funded by NIJ.

The North Charleston Police Department and the Charleston County Aviation Authority Police Department participated in a training scenario during the testing and provided insight and evaluation. RDS, a completely wireless system, uses both radio-based and cellular-based sensors to detect gunfire. Designed for short-term use by an agency (such as during a dignitary protection assignment or a planned response to an alert of continued firearm violence in a specific area), the gunshot detection and location technology uses an array of sensors and a software triangulation program to alert a dispatcher or patrol officer who has the monitoring system in his vehicle to the location of gunfire.

This technology’s main goal is to enable law enforcement to respond more quickly to gunfire-related offenses. In addition, it can serve as an investigative aid to detectives when a victim is shot. The system provides time, date, and location of the incident, as well as an audio file and map of the location. This information can help detectives determine the accuracy of witness accounts.

For more information, contact Ed Hokin of NLECTC–Southeast at 843–750–4625.

**Picture Imperfect**

**Sensors, Surveillance, and Biometric Technologies Center of Excellence**

(Adapted From The New York Times, March 8, 2008)

In a controlled experiment at a Manhattan laboratory, a camera captures a facial image and after preliminary analysis, identifies the face as male. Next, a meter displaying various emotional sensations that the system can recognize appears on the screen below the image. Finally, a second camera conducts a spatial analysis by measuring distance between features such as eyes, ears, cheekbones, and mouth. From the information captured by both cameras, the system builds a composite and runs it against other facial images in the database.

This analysis shows the subject has a 51-percent probability of matching another person in a database, but does not make a positive match. The volunteer subject had not been scanned by the system previously. Facial recognition capable of long-distance image capture and analysis is a highly sought after, but still elusive, technology. This type of recognition, if it ever becomes truly functional, could scan large crowds or individual faces one at a time in a technique known as mass covert data capture.

This exercise was conducted in March 2008 in the controlled environment of a lab operated by International Biometrics Group, which tests biometric technologies and manages the Sensors, Surveillance, and Biometric Technologies Center of Excellence (CoE) on behalf of NIJ. For more information on the CoE and its program, visit [http://www.nlectic.org/coe_surveillance/](http://www.nlectic.org/coe_surveillance/).

New and Improved CSI Help for First Responders

**National Institute of Justice**


Topics include:
- Types of electronic devices commonly encountered at crime scenes and their potential as evidence.
- Investigative tools and equipment recommended for collecting, packaging, and transporting electronic evidence.
- Securing and evaluating a crime scene, including an outline of steps necessary to ensure the safety of all individuals at the scene while protecting evidence integrity.
- Guidelines for documenting a scene.
- Evidence-collection procedures.

NIJ Redesigns Website

**National Institute of Justice**

The National Institute of Justice has redesigned its website to make it easier for users to understand how research can help them shape policy and improve practice.

The new site offers:
- Hot issues of the day on the homepage.
- An “I want to...” section that makes it easier to find answers to common questions.
- Ability to search, e-mail a friend, and produce printer-friendly copies from every page.
- Easier ways to find favorite topics.

The redesign also updated NIJ’s Technology and Tools section with clearer presentation of how NIJ develops and manages its science and technology portfolios, which include:
- Aviation technology.
- Biometrics.
- Body armor.
- Communications technology.
- Electronic crime.
- Less lethal technologies.
- Research and development process.
- Developing technology standards.
- Equipment testing.
- Technology assistance.

NIJ creates new pages all the time. Check back often, and provide input at [http://nij.ncjrs.gov/asknj/](http://nij.ncjrs.gov/asknj/).

Everything You Need To Know About Forensic DNA

**National Institute of Justice**

Explore [www.DNA.gov](http://www.DNA.gov), the website of the President’s DNA Initiative—Advancing Justice Through DNA Technology.

On DNA.gov, users can find free, self-paced online training for law enforcement officers and investigators, officers of the court, and forensic analysts. Some agencies are using the law enforcement training to meet training requirements.
Offering no-cost assistance to law enforcement and corrections agencies and crime laboratories—large or small, rural or urban—in the implementation of current and emerging technologies, the National Law Enforcement and Corrections Technology Center (NLECTC) System is an integrated network of centers, specialty offices, and criminal justice technology Centers of Excellence located across the country.

Established in 1994 by the Office of Justice Programs’ National Institute of Justice (NIJ) as part of its research, development, testing, and evaluation initiatives, the NLECTC System serves as an “honest broker” for technology information and assistance and helps introduce technologies into practice within the criminal justice community.

The NLECTC System seamlessly delivers its expertise to the Nation’s 19,000-plus police agencies; 50 State correctional systems; thousands of prisons, jails, and probation and parole departments; and crime laboratories in a number of technology areas. These technology areas are supported by technology partners who provide the leveraging of unique science and engineering expertise. In addition, technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for NIJ’s various technology focus areas and ensure a focus on the real-world needs of public safety agencies.

Contact NLECTC for:

Technology Identification
The NLECTC System provides information and assistance to help agencies determine the most appropriate and cost-effective technology to solve an administrative or operational problem. We deliver information relating to technology availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability.

Technology Assistance
Our staff serves as proxy scientists and engineers. Areas of assistance include unique evidence analysis (e.g., audio, video, computer, trace, and explosives), systems engineering, and communications and information systems support (e.g., interoperability, propagation studies, and vulnerability assessments).

Technology Implementation
We develop technology guides, best practices, and other information resources that are frequently leveraged from hands-on assistance projects and made available to other agencies.

Property Acquisition
We help departments take advantage of surplus property programs that make Federal excess and surplus property available to law enforcement and corrections personnel at little or no cost.

Equipment Standards and Testing
We oversee the development of performance standards and a standards-based testing program in which equipment such as ballistic- and stab-resistant body armor, double-locking metallic handcuffs, and semiautomatic pistols is tested. NLECTC also conducts comparative evaluations (testing equipment under field conditions) on patrol vehicles; patrol vehicle tires and replacement brake pads; and cut-, puncture-, and pathogen-resistant gloves.

Technology Demonstrations and Capacity Building
We introduce and demonstrate new and emerging technologies through special events, conferences, and practical demonstrations such as the Mock Prison Riot™ and an annual public safety technology conference. We also provide hands-on training assistance for the latest technologies through workshops and software programs dealing with crime mapping, community corrections, and critical incident management. In addition, on a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Technology Information
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, product information databases, news summaries, meeting/conference reports, videotapes, and CD-ROMs. Most publications are available in electronic form through the Justice Technology Information Network (JUSTNET) at www.justnet.org. Hard copies of all publications can be ordered through NLECTC’s toll-free number, 800-248-2742, or via e-mail at asknlectc@nlectc.org.

In September 2007, the U.S. Department of Justice, Office of Justice Programs, created four Technology Centers of Excellence (CoEs) as part of the NLECTC System. Establishment of these CoEs within the existing NLECTC System will further the mission of NIJ by better aligning the NLECTC System with NIJ’s research, development, testing, and evaluation activities, enhancing the cost-effective delivery of technology information and assistance services required by State and local public safety practitioners.

The existing NLECTC sites will continue to serve as the initial point of entry for technology information and generalized technology assistance. The new CoEs will serve as an authoritative resource within their respective technology focus areas, providing specialized technology assistance to public safety personnel as well as working with technology developers and users to test and evaluate equipment in operational environments.

Technology Commercialization
Our law enforcement and corrections professionals, product and commercialization managers, engineers, and technical and market research specialists work together to identify new technologies and product concepts. They then work with innovators and industry to develop, manufacture, and distribute these new, innovative products and technologies.
Attacks or accidents involving chemicals, biological agents, or radiation are likely the most dangerous a law enforcement officer can face. The protective equipment that officers rely on in such incidents must meet the highest standards.

**Equipment Performance Standards**

Existing performance standards for such equipment serve other first responders well, but a law enforcement officer’s mission requires different performance requirements for chemical, biological, radiological, and nuclear (CBRN) protective equipment.

To address that need, the law enforcement community asked the Office of Justice Programs’ National Institute of Justice (NIJ) to develop a standard specifically for CBRN protective equipment used by law enforcement officers. The standard will focus on protective ensembles designed to provide full-body protection against exposure to CBRN hazards. When completed, the standard will be published by NIJ.

**Collaborating With Partners**

NIJ has been working closely with the National Fire Protection Association (NFPA) and the U.S. Departments of Homeland Security (DHS) and Defense (DoD) to leverage related efforts where possible to expedite release of the new NIJ standard.

In August 2007, NIJ organized a special technical committee composed of subject matter experts, many of whom are members of the law enforcement community. Other agencies represented include NFPA, the National Institute of Occupational Safety and Health, DHS, DoD, the FBI, the Drug Enforcement Administration, the International Association of Chiefs of Police, the Fraternal Order of Police, the National Tactical Officers Association, the National Sheriffs’ Association, and organizations that test and certify personal protective equipment.

The committee identified the specific needs and requirements of law enforcement and shortfalls in existing equipment standards and test methods, such as auditory requirements and ergonomic tests. The committee is addressing these shortfalls, determining conformity assessment requirements, and generating a new CBRN ensemble standard.

For more information, contact Debra Stoe, program manager, 202-616-7036, debra.stoe@usdoj.gov; Vanessa Castellanos, program support, 202-353-3182, vanessa.castellanos@usdoj.gov; or Casandra Robinson, program support, 202-385-2596, casandra.robinson@usdoj.gov.