Crime prevention has a new set of eyes to help guard the U.S.-Mexico border. The Eagle Pass Police Department is using a sophisticated new camera system to monitor an area of Texas’ Rio Grande notorious for illegal border crossings and drug smugglings. In its first 6 months of operation, the camera system known as the Eagle Eyes Project has proven itself. Practically no one uses the crossing any more. The success of Eagle Eyes can be discussed as much in terms of crimes prevented as in mass arrests made.

Although it has been quiet under the Camino Real International Bridge, that was not always the case. As Police Chief Juan Antonio Castaneda explains, before the cameras, officers on routine patrol often encountered groups of 40, 50, or even 60 illegal immigrants heading for the downtown area from the river crossing. Since the cameras have been installed, the illegal crossings have dwindled to almost none, a big change from the days when the U.S. Border Patrol caught more than 15,000 migrants from Central America and Brazil crossing in the Eagle Pass area in an 8-month period (“Non-Mexican illegal entrants swamp Texas border,” Arizona Daily Star, May 31, 2005). In addition, several individuals have drowned while attempting to cross the river, and Border Patrol agent Jefferson Barr was shot and killed in the heavily trafficked area in 1997.

“Since the installment of the cameras, we have seen a significant drop in immigration and narcotics traffic,” Castaneda says. “I think the extensive publicity it received in the local media and in the Mexican media has helped discourage people. The area was used extensively by illegal immigrants because the river is very shallow right there; they can literally walk across. Also, the downtown area is very close, and they would run and mingle with the local crowds and disappear.”

According to Castaneda, the cameras also cover a highway heavily used by trucks that runs under the bridge, which connects Eagle Pass with Rio Piedras, Mexico. Hijackings of vehicles by perpetrators coming out of the water had been a concern, but not now.

Eagle Pass obtained the sophisticated surveillance system with the assistance of the Border Research and Technology Center (BRTC), a program of the Office of Justice Programs’ National Institute of Justice (NIJ). Castaneda is familiar with NIJ and its programs. He has been a long-term member of BRTC’s regional advisory council and served as its chair in 2004 and 2005.

“I have been very outspoken over the years about the lack of technology and personnel to combat immigration and narcotics problems,” Castaneda says, adding that Chris Aldridge.

A Different Reality

The training scenario seems all too real. Using a desk for cover, a police officer slowly enters the room, keeping his eyes on the man crouching down in the corner. Suddenly, another man appears, darting around a corner of a cubicle divider and firing his gun at the officer. With only a split second to decide, the officer fires on the second man, bringing him down and causing the first man to drop his gun in surrender.

The room, the desk, the dividing wall—they all stay in place as the officer removes his training gear. The suspects vanish completely.
The room and its contents are real. The two suspects are not. All are a part of the Augmented Reality Training System for Close Quarters Combat scenario, developed by Sandia National Laboratories.

Movies and television have familiarized most people with the concept of virtual reality, which is an artificial environment created with computer hardware and software. To enter a virtual reality, a user wears special gloves, earphones, goggles, and a full-body wiring. In addition to feeding sensory input to the user, the devices monitor the user’s actions. The goggles, for example, track how the eyes move and respond accordingly by sending new video input.

Augmented reality, however, combines an actual physical environment (room, desk, and divider as in the above example) with virtual components (the two suspects). An augmented reality system allows a participant to move around a physical setting and play out a scenario in real time. It enables multiple participants to interact in a three-dimensional environment and adds training in tactical movement and decisionmaking to training in firearms skills. The simulated humans, known as avatars, can hide and dart out, crawl on the floor, and engage in other intelligent behaviors.

“The avatars can do everything but talk,” says Ray Page from Sandia, which developed the state-of-the-art system with funding from the U.S. Department of Energy (DOE)’s Office of Health, Safety and Security.

“You can have gunfights, you can give them voice commands,” Page says. “You can walk 360 degrees around them. The only thing you can’t do is handcuff them—because they don’t exist. I’ve seen guys walk over and touch them after they shot them, which can be funny to watch if you’re not geared up.”

According to Page, being “geared up” consists of nothing more than wearing a helmet and a backpack with a laptop computer and carrying a computer mouse disguised as a weapon.

“When you pull on the weapon’s trigger, you’re actually clicking on your mouse,” he says. “The helmet includes a camera that records what the participant sees for playback and review at the end of the scenario. The overall simplicity of the system means it potentially could be set up in a variety of locations.”

Page came up with the idea for the training program after seeing a demonstration of augmented reality technology several years ago. He approached the Office of Health, Safety and Security’s Office of Technology for funding. DOE and the U.S. Department of Defense’s Technical Support Working Group agreed to jointly fund the prototype, for which Sandia provided the technical development. The project team tested the prototype during 2006 at DOE’s Emergency Operations Training Academy in Albuquerque, New Mexico, inviting various security and law enforcement agencies to view demonstrations and evaluate the system.

Among those viewing the demonstrations was Chris Aldridge, director of the Border Research and Technology Center (BRTC)-Western Operations, a program of the Office of Justice Programs’ National Institute of Justice (NIJ). Aldridge realized that even though the system had been developed primarily for training Federal Government security forces, it had potential for use by State and local law enforcement. Aldridge reported his findings to NIJ after participating in a review of Sandia’s “Work for Others” programs, which provide technical resources and facilities to a variety of other Federal agencies (see www.sandia.gov/bus-ops/partnerships/ways/federal/index.html).

Aldridge subsequently obtained approval to allocate BRTC resources in support of this Sandia effort and arranged for a demonstration of the augmented reality technology to a group of law enforcement professionals and to NIJ’s Modeling and Simulation Technology Working Group last fall. Response was so overwhelmingly favorable that Aldridge worked on obtaining additional NIJ funding designated to develop law-enforcement-specific scenarios.

“The big difference we saw [between this and other similar systems] came in how you can interact with the environment and involve multiple players,” Aldridge says. “I thought this was a great example of how a system developed for another Federal agency could be leveraged into something that could help State and local law enforcement as well.”

He adds that the BRTC-and NIJ-sponsored groups were just two of many providing feedback to help improve the system.

“What all the groups seemed to like the most,” Page says, “was the interaction with the avatars, plus the way you can see everything that is present in the real world and the way you work together as a team. If we’re both wearing the equipment, if you shoot someone, I see it.

“What they didn’t like was the lack of recoil on the weapon, because you’re really just clicking the mouse when you pull the trigger. It didn’t feel right to them, so we’re putting the recoil back on the firearms. They would also like more of a scope-type site.”

DOE also has enhancements in mind, including expanding the capacity from its present 4 users to as many as 15, according to Page.

“It’s hard to get people out once they’re under the helmet,” he says. “They keep saying, ‘give me another one, give me another one.’ What we’d like to do, eventually, instead of just setting it up in a single room, would be to do a whole facility including hallways and then possibly expanding it outdoors. I’d love to see this in operation for a while.”

Present plans call for two fully operational systems to be up and running by October 1, 2007, one in the DOE training academy in Albuquerque and another at a National Nuclear Security Administration operational facility. Sandia, which does not commercialize the technology it develops, is also looking for a partner to bring the product to the open market, potentially sometime in 2008.

Aldridge says that when the system is available commercially, it is likely to be used at regional law enforcement training academies and other similar institutions because he believes the actual cost will be beyond the budgets of most State and local law enforcement agencies.

For more information about the Augmented Reality Training System for Close Quarters Combat, contact Ray Page, rpage@sandia.gov or 505-844-7100.
director of BRTC–Western Operations, saw him being interviewed on C–SPAN several years ago and asked him to serve on the advisory council. His position on the council eventually led to Eagle Pass becoming the demonstration site for the sophisticated surveillance system, dubbed Eagle Eyes in the city’s honor.

The video surveillance system was developed by a team from the University of California–San Diego with funding from the Technical Support Working Group. BRTC had received a request from the Eagle Pass Police Department for assistance in locating this type of technology, and knew that a demonstration site was needed to evaluate the camera system. BRTC introduced the interested parties and helped with obtaining NIJ funding for the cameras installed in Eagle Pass.

The system includes three cameras providing 24/7 coverage, one a stationary unit with a 360-degree view that covers the bridge itself, nearby pedestrian and railroad bridges, local roads, and the riverbank. Two pan-tilt-zoom cameras, one with infrared for nighttime vision, can be focused on specific areas at an officer’s discretion and help triangulate the location of an incident. If the system itself detects unusual movement, it will immediately flag the video stream. Observers can also zoom in on anything they think appears suspicious, record details such as license plate numbers, and dispatch officers to the scene if the situation appears to require it. In the event of a traffic accident, dispatchers know the extent of damage and injuries and can send appropriate help.

“It is wonderful to see this advanced science and technology assisting the people of Texas,” Aldridge says. “We believe this demonstration project will become a valuable platform that can be adapted by other law enforcement agencies charged with protecting our bridges and borders.”

Castaneda is content to have the project remain successful through deterrence, and to that end he periodically contacts the Mexican media for “reminder” articles to keep the system well publicized.

“The problem is under control in this particular area,” he says, adding that Texas Governor Rick Perry is very big on technology and has talked about placing surveillance cameras at numerous sites along the border. The U.S. Border Patrol also monitors some sites. “I’m very big on this technology aspect. It certainly has worked for us.”

For more information about the Eagle Eyes Project, contact BRTC–Western Operations, bRTCwestops@ sbcglobaLnet or 619–229–2277.
Less Than Lethal?

An NIJ study titled Death Following Electro-Muscular Disruption is under way, with findings expected in 2008. The study, which began last year, aims to promote understanding of whether conducted energy device (CED) technology can contribute to or cause death, and if so, in what ways. NIJ initiated the study because an increasing number of police departments are adopting CED devices, commonly called tasers, as a part of their use-of-force continuum. At the same time, the number of deaths reported subsequent to law enforcement agencies’ use of CED technology has increased.

The study’s steering group is co-chaired by NIJ’s deputy director for science and technology and the president of the National Association of Medical Examiners, and includes representatives from the Centers for Disease Control and Prevention and the College of American Pathologists. A panel of physicians is conducting autopsies and toxicological analysis are being combined with evidence from on-the-scene investigations, post-exposure symptoms, and post-event medical care. Panel members also will assess any diseases subjects may have had that could have been contributing factors.

NIJ also is partnering with the International Association of Chiefs of Police to conduct related field research to help reconstruct the chain of events occurring before each death. In addition, field researchers will gather data on in-custody deaths in which there was no prior CED involvement and on cases in which an officer used a CED but no death occurred. By comparing similar cases with different outcomes, NIJ expects to determine whether the use of an CED did, in fact, contribute to those deaths.

For more information on the CED study projects and other less-lethal technologies research at NIJ, contact Joe Cecconi, 202–305–7959.

The Perfect Picture

Typically, video captured on retail surveillance cameras is of poor quality. Analog cameras lack the quality of even home camcorders, digital cameras overcompress the images, and surveillance camera operators may use the same tapes again and again and fail to perform routine maintenance.

But a new software tool that recently received commercialization assistance from the Office of Law Enforcement Technology Commercialization (OLETC) in Wheeling, West Virginia, enhances video images and produces print-friendly still images for use in law enforcement investigation. It also can take a series of multiplexed images (a video stream created by flipping quickly from one camera view to another) and put them in their correct sequence, and can take quadrascene footage (taken simultaneously from multiple camera angles) and break it up into the correct sequence seen from each camera. Users can track an object’s stream of motion by highlighting and then following it through each frame.

The portable tool is compatible with all video cameras on the market. It features user-friendly drag-and-drop editing, point-and-click frame selection, easy frame-to-frame navigation, and intuitive menus. Training time is minimal. Cost of the system ranges from $8,000 to $25,000, depending on whether the user wants the off-the-shelf version or wants to add features customized for the department.

In addition, OLETIC recently provided commercialization assistance to a company that has developed both an artifact and a signature scanner to detect the use of steganography on suspect computers. The artifact scanner tells users whether a suspect has been using steganography software, and the signature scanner locates the hidden data.

Steganography is a method of using computer software to embed hidden text and images inside other files and then transfer the information via the Internet. Terrorists and other criminals often use this method to pass illicit information.

For more information about these resources, contact OLETIC at 888–306–5382.

Cyberthreat Resource Kit

NLECTC—Northeast’s CyberScience Laboratory (C-Kit) is distributing an innovative repository of information that provides wireless and digital forensics resources in a portable, easy-to-access format. The laboratory created this CD-ROM, titled Cyberthreat Resource Kit (C-Kit), in response to numerous requests for assistance from State and local law enforcement to identify technology and tools that can assist in cybercrime investigations.

C-Kit contains wireless security and digital forensic resources that include links to relevant websites, freely distributable software, technical reports, and functional analysis reports. Also on the CD are training videos and presentations that cover forensic tool use and applicability, data-hiding techniques, and potential threats to cybercrime investigations. C-Kit also provides users with a feedback form for comments and suggestions. Based on user requirements and feedback, CSL plans to make future versions of C-Kit available.

(See TECHshorts, page 10)
The National Law Enforcement and Corrections Technology Center (NLECTC) system, a program of the Office of Justice Programs’ National Institute of Justice (NIJ), offers no-cost assistance in helping agencies large and small implement current and emerging technologies. The NLECTC system was established in 1994 by NIJ’s Office of Science and Technology to serve as an “honest broker” resource for technology information, assistance, and expertise by providing information and technology assistance to the Nation’s more than 18,000 police departments; 50 State correctional systems; thousands of prisons, jails, and parole and probation departments; and other public safety organizations.

With a network of regional centers and specialty offices located across the country, the NLECTC system delivers expertise in a number of technologies in partnership with a host organization. In addition, a number of technology working groups and a national advisory council provide guidance relating to the technology needs and operational requirements of the public safety community for each of NIJ’s technology focus areas.

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 serve 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 surplus or property available to law enforcement and corrections personnel at little or no cost.

Equipment Testing
In cooperation with the Office of Law Enforcement Standards (OLES), we oversee the development of test methods 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 on a pass/fail basis. 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. NLECTC has also evaluated emerging products to verify manufacturers’ claims. The primary focus of OLES is the development of performance standards and testing methods to ensure that public safety equipment is safe, dependable, and effective.

Technology Demonstration
We introduce and demonstrate new and emerging technologies through such special events, conferences, and practical demonstrations as the Mock Prison Riot™ (technologies for corrections) and an annual public safety technology conference. On a limited basis, NLECTC facilitates deployment of new technologies to agencies for operational testing and evaluation.

Capacity Building
We provide hands-on demonstrations of the latest technologies to address such operational issues as crime and intelligence analysis, geographic information systems, explosives detection and disablement, inmate disturbances and riots, and computer crime investigation.

Technology Information
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, news summaries, meeting/conference reports, videotapes, and CD-ROMs. NLECTC also publishes TechBeat, an award-winning quarterly newsmagazine.

Because most of the country’s law enforcement and corrections services are provided at the local level, the NLECTC system is composed of five regional centers and is complemented by several specialty offices and a national center: Most centers and offices are colocated with or supported by federally funded technology partners so they can leverage unique science and engineering expertise.
A disaster or critical incident often requires the assistance of emergency responders from different disciplines and jurisdictions that use different radio frequencies. These emergency responders need to coordinate their operations—especially when time is precious and direct radio-to-radio voice communications are essential.

The most basic interoperability solution is to swap radios. One agency loans its radios to personnel from other agencies at an emergency scene. The most sophisticated solution—and the one that provides the greatest level of interoperability—is to build a shared system, also called a shared network, which is a single, large-scale system that serves multiple agencies and often multiple jurisdictions and is designed to meet their collective requirements. This approach is costly, but the participants share the expense.

There is, however, another solution—gateways.

Gateways can deliver an intermediate level of interoperability. They require only minor modifications to existing radio infrastructure and cost much less than shared systems, which normally require purchasing new equipment but may require replacing entire systems and building new towers. Gateways range in capability from simple devices that link two radio channels to highly advanced systems that can interconnect hundreds of devices operating on assorted public safety bands and can simultaneously interconnect trunked talk groups, encrypted networks, the public telephone network, cell phones, and satellite transmissions.

Interconnect devices are gateways that operate by receiving a transmission from one radio system and automatically retransmitting the signal on a different system. They are deployed as fixed-site, mobile, and portable units.

Fixed-site deployment is the generally accepted approach for providing continuous interoperability in a large geographical area when cost or other reasons rule out building a shared system. For example, a fixed site would be appropriate for law enforcement agencies with overlapping or adjacent jurisdictions. The equipment is usually capable of interconnecting a variety of signal sources, routinely including radio, public telephone, and VoIP (Voice over Internet Protocol) transmissions. The most powerful and sensitive equipment, which may demand hundreds of watts, can be used at fixed sites because commercial power lines supply the needed electricity. A disadvantage is that licensing radio channels is more restrictive for fixed sites.

Mobile interconnect devices are designed to be mounted in a vehicle, such as a police cruiser, fire truck, or van serving as a mobile command post. These devices, which often have many of the capabilities of fixed-site equipment, run on the power supply of the vehicle itself and usually transmit at 3 to 110 watts.

Portable interconnect devices are small, light-weight units that can be easily carried or transported by users. As their size suggests, they tend to be less powerful and have fewer capabilities than mobile devices. They are usually designed to operate on both rechargeable batteries and external electric sources.

Mobile and portable devices are deployed to provide temporary interoperability at the scene of a major incident. The incident may involve a relatively small area, such as a tunnel in which an explosion occurred, or a large area, such as thousands of mountainous acres in the throws of a forest fire. Once the equipment is set up, which takes only a few minutes, it will provide interoperability for the duration of the incident. For incident commanders, these devices are valuable tools.

But as important as mobile and portable interconnect devices can be during an incident, there are limitations. One of these limitations stems from the fact that radio spectrum is a limited resource, says Charles Stephenson, public safety communications systems engineer for CommTech (Communications Technologies) and the National Law Enforcement and Corrections Technology Center-Southeast, both programs of the Office of Justice Programs’ National Institute of Justice.

“Radio channels are very tightly controlled by either the Federal Communications Commission for State and local agencies or the National Telecommunications and Information Administration for Federal users,” Stephenson says. “Each channel is licensed to an agency for its use over a fixed geographical area. An area may be very small, such as one that covers a town, or it may stretch across the entire country, as is the case with the channels authorized for use by the U.S. Forest Service. This approach to licensing is designed to allow for maximum channel reuse and so promote an efficient use of the spectrum.”

Against this background of licensed channels, Stephenson says, other realities come into play. First, a large number of interconnect devices are in use. Second, their deployment risks using spectrum inefficiently because of the way they work. Specifically, activation requires a dedicated channel on each interconnected radio system for the duration of the incident and simultaneously increases call traffic on all participating systems when any user is transmitting.

Raymond J. Hayling II, chief public safety communications officer for New Jersey, sent a team to New Orleans to help with hurricane recovery in 2005. He cites the situation as an example of the problems that can occur when interconnect devices are inadequately managed.

“During [Hurricane] Katrina,” Hayling says, “various agencies with interconnect devices converged on the affected areas, and they proceeded to patch radio channels together. Many times, these agencies were unaware of other agencies attempting to use...
the same channels. The interconnect devices further complicated the issue by occupying multiple channels in an uncoordinated fashion. This resulted in an overcrowded and unmanageable mess and almost no communication."

Of course, when many agencies arrive on the scene during any disaster, there is an intrinsic potential for communication trouble from ordinary radio equipment. The mass of responders may soon overload the interoperability frequencies set aside for emergency response personnel. Also, a team may bring equipment that is programmed to operate on channels in their home area and unknowingly interfere with another agency that is licensed to use those channels in the disaster area.

“When it comes to interconnect devices, if their use is not tightly controlled, you can easily end up with multiple devices connecting the same channels together, potentially making unusable whatever channels are connected,” Stephenson adds.

Technologically, interconnecting channels with these devices is fairly easy, but to avoid overwhelming the linked channels with intermixed and incompatible radio conversations, agencies ought to have carefully conceived plans delineating rules of operation and device management. Furthermore, device management is such a critical function that it should be handled by trained staff, especially when more than one device is operating in the area or at the incident scene. Trained device managers are also important when encryption is involved, for encrypted communications can be inadvertently retransmitted over an unencrypted link without the intended encryption.

In New Jersey, Hayling says, interconnect devices are generally restricted to use during critical incidents when more than one agency is involved. Additionally, the State interoperability plan includes a device-alert mechanism that helps system managers coordinate the use of these devices and avoid communication problems.

"All devices used by public agencies in New Jersey have voice ID," Hayling says. "Each announces itself as an interconnect device and states its identification number in plain English. All are also equipped with special antenna ports to connect with in-building and in-tunnel systems by cable if an interconnect device is needed to improve outside-inside communication."

Instituting rules of operation and assigning trained staff to manage these devices are recommendations that can eliminate or minimize deployment problems. Still, some organizations have chosen to bypass potential problems by banning the equipment. Stephenson notes that several large agencies across the country do not allow the use of interconnect devices on their systems. “For instance,” he says, “I have worked a lot with the agencies around Boston, and their use in that area is largely prohibited.”

For more information about interoperability, gateways, and interconnect devices, visit the CommTech homepage at www.ojp.usdoj.gov/nij/topics/technology/communication/welcome.htm. Additional information resources include the Guide for the Selection of Communications Equipment for Emergency First Responders and the Guide to Radio Communications Interoperability Strategies and Products, which can be accessed, along with other systems planning and management documents, through the U.S. Department of Homeland Security’s SAFECOM website at www.safecomprogram.gov/SAFECOM/library/systems.

One type of interconnect device is the ACU–1000, a switch that can interconnect dissimilar radio systems. The ACU–1000 allows wireless communication systems to be combined at the audio baseband by using the received audio from one radio system as the source audio.

The interconnect device was developed privately and extensively tested in an operational setting with assistance from the National Institute of Justice, a program of the Office of Justice Programs, which studies interoperability matters through its CommTech (Communications Technologies) program, formerly known as AGILE.

CommTech’s primary objective is to help improve emergency response communications by identifying, examining, and developing interoperability solutions that include open architecture standards for voice, data, image, and video communication systems. When existing technologies fall short, CommTech conducts research to find new solutions.

The program also aims to raise awareness of interoperability issues through outreach programs so policymakers and emergency response leaders can make informed and cost-effective decisions.
Drinking. Doing drugs. Driving without a license. Exchanging identities. Common behaviors of paroled and probationed offenders in the community. Common behaviors that nevertheless have been difficult to detect and stop.

Several newly developed technologies may help uncover and curb these behaviors and provide probation and parole officers with tools to better manage their caseloads by doing their jobs more effectively and efficiently.

Three of these technologies were on exhibit during a recent Innovative Technologies for Community Corrections Conference sponsored by the National Law Enforcement and Corrections Technology Center–Rocky Mountain, which is a program of the Office of Justice Programs’ National Institute of Justice (NIJ). This yearly conference showcases various new technologies directed to the corrections field.

Driver Monitoring and Surveillance

This surveillance technology consists of a pair of ankle bracelets that collect data on the unique patterns of movement associated with foot-to-brake, foot-to-gas pedal, acceleration, and deceleration of a motor vehicle. Data analysis can then indicate if and when a subject has been driving. In the case of an individual whose license is restricted, rather than suspended, it can also indicate if the driving took place during a prohibited time (such as outside the normal workday).

The bracelets can store and process data for up to 30 days, allowing a community corrections officer to upload data during a scheduled monthly visit. This technology would help community corrections professionals deal with a widespread and longstanding problem, as research indicates that up to 75 percent of all drivers with suspended or restricted licenses continue to drive.

More information about the system is available through the website of NIJ’s Office of Law Enforcement Technology Commercialization at www.oletc.org/quadcharts.html (click on License Sanction Enforcement System).

Sleep Pattern Analysis

Sleep pattern analysis technology, already used by some jurisdictions, can provide preliminary indications of substance abuse and help community corrections officials determine if more testing is warranted.

Sleep disruption due to substance abuse can occur in several ways, including altering the sequence and duration of various stages of sleep, total sleep time, and the amount of time needed to fall asleep. The technology consists of a small device, secured to an offender’s wrist with a tamper-evident band, that measures sleep quality through recording gross motor activity. Analysis of the data collected may indicate sleep disorders, which potentially could be caused by substance abuse. The device passively collects and records body movement information, and when the offender reports to the probation office or drug court, data can be downloaded and analyzed in a matter of minutes. If data analysis indicates possible substance abuse, the offender can be required to immediately provide a urine specimen for further testing.

Infrared Spectroscopy

Currently in field tests, this technology seeks to modify a glucose-monitoring device into an alcohol-testing product. The device uses a light source, an optical detector, and spectrometers to conduct chemical analysis of tissue and measure alcohol levels. Results, available within just 1 minute, have accuracy comparable to that of breathalyzers and blood tests.

The technology uses infrared spectroscopy to make a nonintrusive examination of a subject’s inner forearm; the device also could be modified to examine other parts of the body. The analysis process incorporates a biometric component that identifies an individual’s unique tissue structure and tissue chemistry, thus ensuring accurate identification of the person being tested.

In addition to producing results quickly, the device can easily be used by a nonmedical professional and thus has potential for use in a probation office, work release center, or even the suspect’s own home or a self-reporting kiosk.

For more information about these and other technologies showcased through the Innovative Technologies for Community Corrections conference series, contact Joe Russo at the Rocky Mountain Center, 800–416–8086 or jrusso@du.edu.
Biometrics is a general term used alternatively to describe a “characteristic” or to describe a “process.” As a characteristic, biometrics refers to anatomical, physiological, or behavioral characteristics that can be used for automated recognition. Signatures and the sound of the voice fall into the behavioral category. Blood type and DNA are physiological characteristics. Anatomical characteristics—such as fingerprints, the iris, hand geometry, and the face—are the most frequently used biometrics because they can be measured quickly and easily at a reasonable cost.

As a process, biometrics refers to automated methods of recognizing an individual based on measurable anatomical, physiological, or behavioral characteristics. Biometric (process) systems typically have five components:

1. A sensor for capturing and digitizing data from enrollees.
2. Processing algorithms for forming biometric templates.
3. A unit for storing data and templates.
4. Matching algorithms for comparing new templates with the stored templates.
5. A decision process for accepting or rejecting individuals.

Three main kinds of errors are used to rank the performance of biometric systems:

1. The failure-to-acquire rate is the percentage of times a system fails to capture a useful biometric from an individual.
2. The false-accept rate is the percentage of times an individual is incorrectly matched to the template of another individual.
3. The false-reject rate is the percentage of times an individual is not matched to the individual’s existing template.

Biometric technologies have indisputable advantages for establishing and verifying identity. No one can forget biometric characteristics, lose them, or give them to someone else. Additionally, they are either unchangeable or highly resistant to being changed. In recent years, biometric technologies have become better, faster, easier to use, and cheaper. The number of law enforcement and corrections biometric applications is growing rapidly. Potential users should learn as much as possible about the technology and systems to ensure they produce good results.

Five Leading Biometric Technologies

**Fingerprint readers** capture an image of a fingerprint, extract a pattern, and mathematically encode the pattern into a template representing the image. Optical devices capture samples using light and are the only ones designed with enough sensor area to capture the fully rolled fingerprints needed for FBI identity checks; processing all 10 fingers makes operating speed slow. Capacitive devices, usually designed to require one fingerprint, detect the electrical field where a finger touches the sensor; these readers are fast, compact in size, less expensive, and typically used for access control. Fingerprint readers are the most popular biometric devices (nearly 80 percent of the world market), and huge databases of print images are available. False-accept rates are less than 1 in a million; false-reject rates may be more than 2 percent.

Optical devices use several methods, but basing identification on minutiae points (where print ridges begin, terminate, or split) is the most popular. A fingerprint typically has 30 to 40 minutiae. (The FBI finds that no two individuals have more than eight minutiae points in common.)

**Iris recognition technology** captures the image of the iris using a high-quality digital camera. Its complex pattern is converted using algorithms into a 512-byte template called an IrisCode®, invented and patented by Dr. John Daugman in 1994. Scanning can be done from a few inches to a yard away and takes just seconds; the small template allows a database to be searched rapidly. Tests show that iris scanning has a false-accept rate of 0.1 percent, with a false-reject rate of 1 to 2 percent.

A disadvantage of the technology is that no huge database exists (such as the FBI’s for fingerprints). In addition, one cannot leave an iris “print” at the scene of a crime and failures to acquire a good iris image may be as high as 10 to 15 percent in bright outdoor lighting, although training usually lowers that percentage.

The iris structure is set by age 1 and appears to remain the same throughout life. The iris is like a human barcode: No two are the same.

**Face recognition technology** captures the image of a face with a camera and constructs a template. Early face recognition algorithms used simple geometric models, but the recognition process has matured into a science of sophisticated mathematical representations and matching processes. Major advances in the past 10 to 15 years have made the use of face recognition more common. The technology is now used both to verify a claimed identity and to identify someone by searching a database for possible matches. A clear advantage of face recognition technology is that images can be captured without physical contact; devices could become valuable surveillance tools. Continuing technical challenges are that systems often cope poorly with changes in lighting or with images taken from the side or above. A shift from low-resolution two-dimensional images to high-resolution two- and three-dimensional images shows potential for improving system accuracy.

(See Biometrics, page 12)
School Watch

The Hollywood (Florida) Police Department has used Secure Our Schools funding from the U.S. Department of Justice’s Office of Community Oriented Policing Services to purchase and install wireless remote video surveillance equipment to enhance the surveillance capability and security measures at South Broward High School, according to Capt. Tom Sanchez, who is in charge of school safety and a member of NIJ’s School Safety Technology Working Group. The department also appropriated about $48,000 in matching funds to support the program.

The system has had marked success in just a few months of use. In several different vandalism incidents, suspects confessed after being shown video from the system. Recently, while a school resource officer was monitoring a home football game on his laptop, he saw three males jump the fence surrounding the school. He radioed for backup and continued tracking the suspects, who were picked up by waiting patrol officers.

South Broward High School was chosen as the city’s demonstration site for the wireless remote surveillance technology based on a large student population and associated issues. The school sits on a 20-acre campus with multiple buildings and is now equipped with 60 security cameras controlled from a single access point inside a camera room. Prior to installation, experts conducted a wireless site survey to determine the location and configuration of the wireless implementation, after which the department purchased an eight-port Ethernet video server along with other support hardware. The server provides 1.5 terabytes of storage and accommodates 30 days of digital video recordings.

The system replaces a room full of fixed video screens, VHS-style recorders, and old tapes needing regular changing. The cameras are connected to video processing units that convert the signal to digital and then send it to the server for archiving. The server sends the signal to a main switch, which sends it to the school network and a wireless access point. From the school network, school administrators can view the video feed from their office computers. Monitoring can also be done via personal digital assistants, allowing the school resource officer to monitor the cameras while conducting other functions. Officers can also view any of the school’s surveillance cameras from their in-car computers while within the outer perimeter of the school. Multiple cameras can be monitored at the same time from these laptops, and previously recorded events can also be retrieved. In addition, each officer’s laptop contains safety plans with aerial and ground pictures, floor plans, maps, and other information on every school.

For additional information about the South Broward High School security initiative or the School Safety Technology Working Group, contact NLECTC–Southeast, 800–292–4385 or nlectc-se@nlectc.org.

N o-cost software is available to help school officials analyze and map incidents that occur in or near schools. Developed by Abt Associates in 2000 with funding from the Office of Justice Programs’ National Institute of Justice (NIJ), the School COP software package has been downloaded more than 8,000 times. Thousands of copies of the School COP CD–ROM also have been distributed to school resource officers (SROs) and school administrators at COPS in Schools conferences sponsored by the Office of Community Oriented Policing Services.

School COP is for everyday use and enables SROs, SRO supervisors, school administrators, and security officers to do the following:

• Enter incidents daily, which saves people time in completing required monthly or annual reports.
• Display incidents involving a particular student quickly, which is valuable for meetings with parents or students.
• Produce graphics showing school “hot spots” or year-to-year trends, which can help solve problems and communicate issues at school meetings. For example, a map can show where bullying incidents have occurred on a school campus.
• Provide evidence of activities undertaken or problems solved, which can help persuade a school board to continue funding an SRO program.

Although developed for use in K–12 schools, School COP has been used in other settings. With funding from NIJ, researchers at Temple University modified the package for use in correctional settings, calling it Facility COP. School COP is also being used in post-secondary schools, law enforcement gang and narcotics units, and hospitals (to track security infractions and alarms).

School COP runs on PCs that use Windows 95, 98, NT, 2000, and XP and have at least 16 MB of RAM and 20 MB of available hard disk space.

To receive more information or to download a free copy of School COP, visit www.schoolcopssoftware.com or contact Mike O’Shea, NJ program manager, at Michael.OShea@usdoj.gov. For more information about Facility COP, visit www.temple.edu/cj/faccop. For more information about COPS in Schools sponsored by the Office of Community Oriented Policing Services, go to www.cops.usdoj.gov, click on the News & Events tab, then on Training, and select COPS in Schools Training.

NEW Publication:

2007 Model Year Patrol Vehicle Testing

The purchase of patrol vehicles is one of the largest expenditures that a law enforcement agency faces. Each year, the Michigan State Police and the Los Angeles County Sheriff’s Department conduct extensive evaluation tests on new model year police vehicles. The Office of Justice Programs’ National Institute of Justice, through its National Law Enforcement and Corrections Technology Center (NLECTC)–National, partners with the two agencies to conduct the tests and disseminate the results to the law enforcement community nationwide.

The report on the results of the 2007 police patrol vehicle testing, which also includes motorcycle testing and a comparison of the Michigan and Los Angeles programs, is now available online and on CD–ROM.

To obtain a no-cost copy of the CD, contact NLECTC–National at 800–246–2742 or visit www.justnet.org.
TechBeat is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. TechBeat’s latest award is the APEX 2006 Award of Excellence—Newsletters–Print. Our goal is to keep you up to date with current and developing technologies for the public safety community, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year.

Individual Subscriptions: TechBeat is available at no cost. If you are not currently on our mailing list, please call us at 800–248–2742; fax 301–519–5149; or e-mail us at asknlectc@nlectc.org.

Domestic Department Subscriptions: If your division, department, or agency has more than 20 individuals, we can drop ship as many copies as you require. All you have to do is provide us with the quantity needed, a shipping address (no Post Office boxes, please), and a contact name and telephone number. Your only obligation is to disseminate them once they arrive. If you require fewer than 20 copies, please provide us with the names and addresses of individuals who are to receive the newsmagazine and we will send copies directly to them. Contact Rick Neimiller, TechBeat managing editor, at 800–248–2742 for additional information or to subscribe.

Address Correction: Please notify us of any change in address or point of contact. Call 800–248–2742; fax 301–519–5149; or e-mail asknlectc@nlectc.org.

Article Reproduction: Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as, “This article was reproduced from the Spring 2007 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the Office of Justice Programs’ National Institute of Justice, 800–248–2742.”

Awards: TechBeat has received numerous awards, including the 1998 Best of Category, Excellence in Printing Award from the Printing & Graphic Communications Association; the first-place 1998 Blue Pencil Award for Most Improved Periodical from the National Association of Government Communicators; the 1999 Silver Inkwell Award of Merit from the International Association of Business Communicators; the APEX 2001 Award of Excellence for Magazines and Newspapers–Printed; and the APEX 2006 Award of Excellence-Newsletters–Print.

Photo Credits: Photos used in this issue of TechBeat copyright © 2007 Getty Images, ShutterStock, iPhotos; and Arresting Images Photo Gallery.

Staff: Managing Editor, Rick Neimiller; Editor, Michele Coppola; Assistant Editor, Janet McN Nugent; Lead Writer, Becky Lewis; Contributing Writer, Vaughn Deckert; Graphic Designers, Cheryl Denise Collins and Tina Kramer.

www.justnet.org

Online News Summary. Online News Summary includes article abstracts on law enforcement, corrections, and forensics technologies that have appeared in major newspapers, magazines, and periodicals and on national and international wire services and websites.

Testing Results. Up-to-date listing of public-safety equipment evaluated through NIJ’s testing program. Includes ballistic- and stab-resistant armor, patrol vehicles and tires, protection gloves, handcuffs, and more.

Publications. Publications from NIJ and NLECTC that you can view or download to your system, including printer-friendly versions of TechBeat articles and features.

Calendar of Events. Calendar of Events lists upcoming meetings, seminars, and training.

Links. Links takes you to other important law enforcement and corrections websites.

For help establishing an Internet connection, linking to JUSTNET, or finding needed technology and product information, call the NLECTC Information Hotline at 800–248–2742.

National Criminal Justice Reference Service

In addition to funding the National Law Enforcement and Corrections Technology Center, the National Institute of Justice (NIJ) and other Federal agencies support the National Criminal Justice Reference Service (NCJRS), assisting a global community of policymakers, practitioners, researchers, and the general public with justice-related research, policies, and programs.

NCJRS offers reference and referral services, publications, onsite and offshore conference support, and other technical assistance. The easiest way to access NCJRS is online.

Start at http://www.ncjrs.gov

The NCJRS website showcases the latest criminal and juvenile justice and drug policy information. Take advantage of:

• Topic-specific resources.
• Online registration and ordering.
• Searchable abstracts, calendar of events, and questions-and-answers databases.

Stay Informed

Register at http://www.ncjrs.gov/subreg.html to receive:

JUSTINFO. A biweekly electronic newsletter that includes links to full-text versions of printed publications.

E-mail notifications. Periodic messages about new publications and resources that match your specific interests.

NCJRS Contact Information at-a-Glance

Web: http://www.ncjrs.gov
Phone: 800–851–3420 (Monday – Friday, 10 a.m. to 6 p.m. E.S.T.)
Fax: 301–519–5212
Mail: NCJRS, P.O. Box 6000, Rockville, MD 20849–6000

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #2005–MU–CX–K077 awarded by the U.S. Department of Justice, National Institute of Justice. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Lockheed Martin. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.
The results of recent Face Recognition Vendor Tests (http://face.nist.gov/FRVT) show that the performance results for face recognition technology are similar to those for iris recognition technology, with a false-reject rate of 0.1 percent and a false-accept rate of 2 percent.

Hand geometry scanners use a CCD (charge-coupled device) camera to capture the dimensions of a hand placed on a plate palm down, guided by five pegs that sense when the hand is in position. Mirrors allow data to be gathered from the side and top of the hand. A scanner takes 90 measurements—such as lengths and widths of the fingers, distances between knuckles, and surface areas—and constructs a template. Enrollment usually requires capturing three images. Verifying that a person is who he or she claims to be involves swapping an identity card or entering a personal identification number right before scanning a subject’s hand for comparison against the stored template; the system generates a similarity score and accepts or rejects the subject. Commercially available since 1986, these devices capture measurements in about 1 second. They are noninvasive, easy to use, reasonably accurate, and highly acceptable to the public. Unlike fingerprint readers, hand geometry scanners are not affected by lines, scars, dirt, and other surface details. This technology serves well for fast, easy, and frequent identity checks—for example, to track the crossings of frequent travelers at borders, to track attendance at workplaces, and to control access in general.

Over time, the shape of the hand does not change significantly, but hand geometry is not unique. Too many hands are similar in size and shape for this biometric to deliver high-security verifications.

Dynamic signature identification systems use software to measure the speed, direction, and pressure of pen strokes while signing an electronic tablet. Enrollment usually requires a set of sample signatures. From the data collected for each feature, the software constructs a digital template for comparison with future signatures. Although a forger can replicate a signature with practice, it is nearly impossible to duplicate how a person writes his or her signature, which makes the dynamic method a reliable biometric. Many patented technologies for signature identification are available, and systems are inexpensive. This biometric, though, is prone to high false-reject rates because signatures may vary from one signing to another. The development of techniques for differentiating the parts of a signature that are consistently the same from those that vary with each signing has reduced error rates.

Because signatures are required in everyday transactions, this biometric has a great advantage: public acceptance.

Editor’s note: DNA matching is a method of recognizing a person based on chemical sequences at specific places along the DNA molecule. This tool for establishing identity and proving guilt or innocence, however, cannot be regarded as a biometric because much of the process is not yet automated.

For more information about biometrics, visit “Introduction to Biometrics” (under “Additional Resources”) and other webpages at www.biometricscatalog.org/defaul.aspx, or contact William Ford at the Office of Justice Programs’ National Institute of Justice, William.Ford@usdoj.gov.

The results of recent Face Recognition Vendor Tests (http://face.nist.gov/FRVT) show that the performance results for face recognition technology are similar to those for iris recognition technology, with a false-reject rate of 0.1 percent and a false-accept rate of 2 percent.

Hand geometry scanners use a CCD (charge-coupled device) camera to capture the dimensions of a hand placed on a plate palm down, guided by five pegs that sense when the hand is in position. Mirrors allow data to be gathered from the side and top of the hand. A scanner takes 90 measurements—such as lengths and widths of the fingers, distances between knuckles, and surface areas—and constructs a template. Enrollment usually requires capturing three images. Verifying that a person is who he or she claims to be involves swapping an identity card or entering a personal identification number right before scanning a subject’s hand for comparison against the stored template; the system generates a similarity score and accepts or rejects the subject. Commercially available since 1986, these devices capture measurements in about 1 second. They are noninvasive, easy to use, reasonably accurate, and highly acceptable to the public. Unlike fingerprint readers, hand geometry scanners are not affected by lines, scars, dirt, and other surface details. This technology serves well for fast, easy, and frequent identity checks—for example, to track the crossings of frequent travelers at borders, to track attendance at workplaces, and to control access in general.

Over time, the shape of the hand does not change significantly, but hand geometry is not unique. Too many hands are similar in size and shape for this biometric to deliver high-security verifications.

Dynamic signature identification systems use software to measure the speed, direction, and pressure of pen strokes while signing an electronic tablet. Enrollment usually requires a set of sample signatures. From the data collected for each feature, the software constructs a digital template for comparison with future signatures. Although a forger can replicate a signature with practice, it is nearly impossible to duplicate how a person writes his or her signature, which makes the dynamic method a reliable biometric. Many patented technologies for signature identification are available, and systems are inexpensive. This biometric, though, is prone to high false-reject rates because signatures may vary from one signing to another. The development of techniques for differentiating the parts of a signature that are consistently the same from those that vary with each signing has reduced error rates.

Because signatures are required in everyday transactions, this biometric has a great advantage: public acceptance.

Editor’s note: DNA matching is a method of recognizing a person based on chemical sequences at specific places along the DNA molecule. This tool for establishing identity and proving guilt or innocence, however, cannot be regarded as a biometric because much of the process is not yet automated.

For more information about biometrics, visit “Introduction to Biometrics” (under “Additional Resources”) and other webpages at www.biometricscatalog.org/defaul.aspx, or contact William Ford at the Office of Justice Programs’ National Institute of Justice, William.Ford@usdoj.gov.