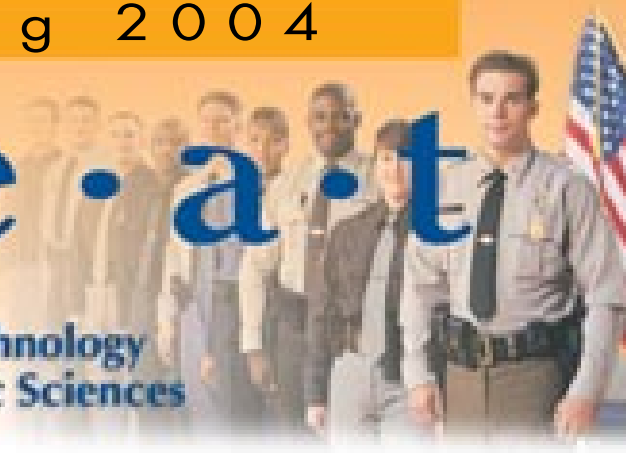
National Law Enforcement and Corrections Technology Center

TECH b·e·a·t

Spring 2004

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences



At the Scene of the Crash

More and more, when it comes to investigating vehicle crashes, distance measuring tapes and wheels, hand-drawn sketches, and ink pens are out and computers and lasers are in.

"The days of going out and measuring skidmarks and using calculus to determine speed are over," says Troy Krenning, a program manager at the National Institute of Justice's National Law Enforcement and Corrections Technology Center (NLECTC)–Rocky Mountain in Denver, Colorado. "These data are now captured in the vehicle's black box."

According to William Mael, a transportation safety consultant in Fort Collins, Colorado, the technology for analyzing vehicle crashes had long remained relatively unchanged. However, Mael says, "Starting about 3 to 5 years ago, much of the technology became computer-related or laser-related, requiring a higher level of training and exposure for law enforcement personnel."

"Onboard vehicle data recorders and other high-tech tools promise to make crash scene investigation faster, more efficient, and more cost effective, but many departments lack the expertise to use them," Krenning says. To help bring law enforcement agencies up to speed on current crash scene technologies, NLECTC–Rocky Mountain last year initiated a technology assistance program titled "Crash Scene Technologies," which is available to law enforcement agencies at no cost.

Last year, Krenning says, approximately 120 officers from Colorado, Montana, and Kansas took the week-long course, a mix of classroom presentations and hands-on exercises designed for experienced crash scene investigators dealing with major accidents. NLECTC–Rocky Mountain also is offering technology assistance in specific areas, such as motorcycle crash analysis and advanced reconstruction techniques. The crash scenes technology course is presented by Mael along with Bob Rood, a Colorado State Patrol specialist in major collision investigations. It presents a broad spectrum of technologies, but without promoting specific products.

"There are probably 10 different companies that make measuring devices and 30 different companies that make computer-aided drafting (CAD) programs for law enforcement," Mael says. "Police agencies are inundated with these things and don't necessarily know how to choose which they want to use."

(See Scene of the Crash, page 10)

Hot Off the Wireless

In a recent television commercial a stressed-out office worker takes his laptop to a park and uses his wireless access connection to meet his deadline as he basks in the warm sunshine. Other television and radio advertisements promote the same message: wireless connections make life more convenient, faster, easier. But these commercials do not mention the hidden dangers that every consumer—and every law enforcement officer—should watch for.

Statistics released by the Federal Bureau of Investigation in 2003 show that "cybercrime" rates increased for the third straight year. Although most people know about financial fraud, identity theft, and the dangers hackers can pose to conventional systems and networks, most are unaware of the unique risks from the use of wireless access technology. Staff at the National Institute of Justice's CyberScience Laboratory (CSL) in Rome, New York, know the risks and want to share this information with law enforcement agencies across the Nation.

Search the Internet for information on wireless technology and you will be overwhelmed by the huge amount of

(See Hot Off the Wireless, page 2)

(Hot Off the Wireless . . . cont. from page 1)

information—some accurate, some not. CSL staff have sorted through that mass of information, applied their technical knowledge and expertise, and produced several primers, an informational DVD, and lists of links to the most useful sites. (These are available by calling the laboratory at 888–338–0584.)

As information technology companies tout wireless use, consumers buy laptop computers and set up wireless access points in their homes and offices without learning about the need for wireless security, says Robert DeCarlo, Jr., an economic crime specialist with CSL. "The vast majority of crimes involving wireless use go undetected and unreported. The victims don't know they're vulnerable, and law enforcement doesn't know the signs to look for. I think we're on the cusp of an explosion of crime using wireless technology."

Jeffrey Isherwood, a CSL senior engineer, says he can recall officers telling him about only one or two cases in which the suspect had wireless access. Ironically, at least half of the officers he talks with tell him they have wireless access in their homes or precincts. Just like the average consumer, these officers are aware of the benefits of wireless use, but not its potential security risks. "Wireless often is the last thing that police think of when someone reports identity theft," Isherwood says. "They ask victims where they've been shopping. If they do check victims' computers, they don't think to ask specifically about wireless."

"It's not that there's a specific crime here; it's a method of perpetrating a crime such as identity theft, and it's a method that's very hard to trace and prove," says Joshua Bartolomie, another CSL electronic crime specialist in wireless issues. "For instance, you might live in an apartment building with 10 apartments and someone might be sitting downstairs collecting all of your information. It's the perfect way to perform identity theft."

Bartolomie also says "WarDrivers" (slang for wireless hackers) drive around and look for wireless networks, hoping to find an open access point in a home or office and break into it or piggyback off it from laptops in their vehicles. They break in, cause problems, and then drive away, leaving no evidence behind.

Isherwood says he and Bartolomie perform test sampling whenever they attend a conference. "We use the same equipment and technology that the hackers use," Isherwood says, "and we get numbers that compare to the nationally reported figures. That is, about 75 percent of all wireless access points are unencrypted and wide open, and anybody who wants to can gain access to them."

For that reason, CSL staff caution that officers need to be alert for such warning signs as occupied cars in office parking lots long after businesses have closed, people using laptops in cars, and WarDriving antennas. According to Bartolomie, potato chip cans are almost the exact width and length needed to create an antenna to handle the frequency range that wireless networks use. All a WarDriver needs to create the antenna is another $5 in parts: "If a cop sees someone with a Pringle's can with wires sticking out of it, ask questions!" he says.

"Commercial versions are also fairly cheap," Isherwood says. "They're about 3 inches tall, with a magnetic base. It's hard to distinguish them from a CB or cell phone

"You might live in an apartment building with 10 apartments and someone might be sitting downstairs collecting all of your information . . .

A Wireless Intro

How does wireless access work?

- Wireless access technology uses radio communication to allow any computer, not only laptops and personal digital assistants (PDAs), to access a network.

Why use wireless?

- Wireless connections allow users to access a network from virtually anywhere: home, car, even the beach. They are easy to install and relatively inexpensive to maintain.

How do you obtain wireless access?

- Many new laptop computers have built-in wireless adapter cards. These cards also can be purchased at almost any electronics or office supply store. Installation is usually simple: As soon as a user plugs them into a computer, the cards will usually connect to the nearest working access points.

What are the security risks?

- It is so easy to set up a wireless local area network (WLAN) that employees may set up access points in their offices without telling their information technology department. Unfortunately, such users may have no knowledge of proper security protocols and procedures.
- All hardware comes with the manufacturer's default settings, which often create access points configured for public access; that is, the newly installed access points are broadcasting "beacon packets" that identify them as available to anyone in the area who is listening. Unfortunately, if cards were manufactured with initial security settings enabled, they might not install easily. Moreover, many users do not know they should immediately reconfigure their access points to restrict access. According to CSL staff, although manufacturers provide information about security risks, few people read it.
- Anyone who has the right equipment can detect and break into open access points. Using a potato chip can or a coffee can and some copper wire, an individual can build a directional antenna having a range of hundreds of yards for very little money.

What basic steps can users take to protect themselves?

- Wireless access points do not require users to log in with a user name and password. Therefore, IT departments should integrate WLANs into their existing infrastructure to provide maximum protection. Access points should be on a segregated network behind a firewall that requires users to be authenticated before they can access the organization's entire network.
- Wireless fidelity (WiFi) equipment comes with wired equivalent privacy (WEP), a built-in encryption algorithm to scramble data. Although the WEP encryption algorithm can easily be broken, it provides some protection, particularly if users change from the default settings.
- Adding a Virtual Private Network will encrypt an entire framed session, not just the data.
- In a wireless network, Media Access Control (MAC) addresses, which identify network interface cards (each of which has a unique number), can be filtered to provide access to known users only.

What is WarDriving?

- WarDriving derives from the term "WarDialing" used in the 1983 movie War Games, in which a teenager used his computer to dial blocks of numbers in search of a way to break into a video game company's systems. It refers to driving, walking, biking, or otherwise cruising around looking for open access points. WarDrivers often use one of many WiFi detection programs available for free from the Internet. Although many WarDrivers do this simply for fun, others have malicious intent. WarDrivers generally

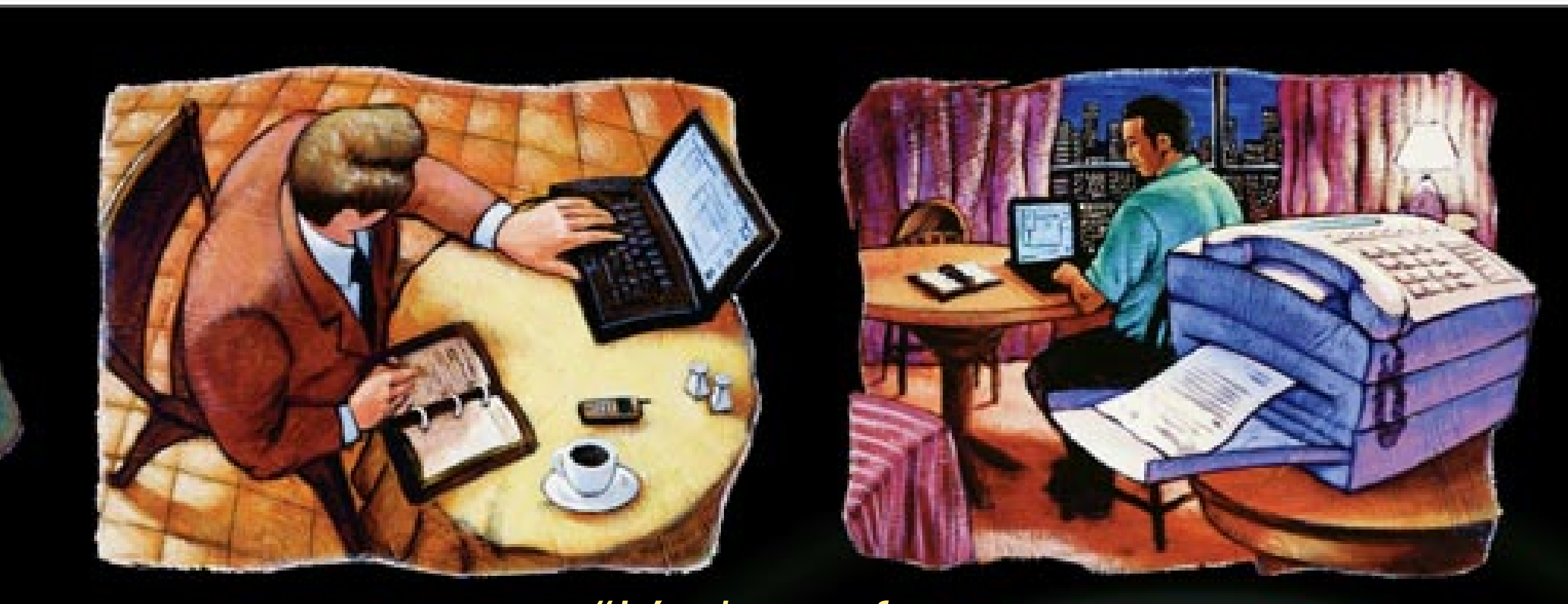
antenna. Officers should also watch for GPS units and/or laptops connected to the GPS, the antenna, or a can. Anyone using a laptop in a car would arouse my suspicions, period, especially if the car is moving."

"If an officer pulls over someone whom they suspect of WarDriving, he or she should note the time and the license number and report it to whoever in their department handles cybercrime issues. It might prove to be useful information a week, or even a month later, because it might take the victim that long to realize something has happened," he adds.

However, these subtle warning signals can be hard to spot. For that reason, CSL staff encourage officers—and consumers—to learn about wireless security and take all the steps they can to safeguard their wireless access. Officers can start by contacting CSL or registering at www.cybersciencelab.com to download *Introduction to Basic Networking, Introduction to the 802.11 Wireless Network Standard,* and *Security Threats to the 802.11 Wireless Network.* These three reports (one of which includes a glossary of basic wireless networking terms) meet the needs of most law enforcement professionals. CSL staff are preparing more advanced documents to supplement these reports.

"We're just interested in getting the information out to State and local law enforcement. If you go to a company website, they're going to plug their products. We're not interested in doing that," DeCarlo says. "We see ourselves as the resource in this area for law enforcement and corrections agencies that need help, and our specialists really know this stuff."

For more information on wireless access and issues, cybercrime in general, or the CyberScience Laboratory, contact Joshua Bartolomie, 315–838–7057 or Josh@DolphTech.Com; Jeffrey Isherwood, 315–838–7064 or Ish@DolphTech.Com; or Robert DeCarlo, Jr., 315–330–2489 or robert.decarlo@rl.af.mil.



"It's the perfect way to perform identity theft."

need to be within 300 feet of equipment to detect a wireless access point, although if they have high-powered antennas at their disposal, they could be miles away.

What is the IEEE?

- The Institute of Electrical and Electronic Engineers (IEEE) establishes standards for wireless use, including the 802.11 set of wireless access standards. Members of this group of academics and technology professionals work together to adopt and refine protocols and operational standards for many types of community technology.

What is the 802.11 standard?

- IEEE has approved three related standards for wireless networking: 802.11a, 802.11b, and 802.11g. (Other standards are in development.) Equipment that meets any of the 802.11 standards falls into the category of WiFi devices. Any equipment carrying the WiFi trademark from the Wireless Ethernet Compatibility Alliance is guaranteed to operate with at least base functionality.
- WiFi uses unlicensed spectrum in the 2.4 GHz range, except for 802.11a, which uses the 5 GHz licensed frequency range. This spectrum originally was left unlicensed so it could be used by microwaves and similar equipment, but many other devices now use this spectrum. The 802.11 standard specifies connectivity at 11 megabits per second (Mbps), compared to 9.6 kilobits per second for older cellular phones. Current phones can connect at hundreds of kilobits per second.
- Most wireless access equipment used in the United States meets the 802.11b standard, operating on a frequency of 2.4 GHz at a maximum speed of 11 Mbps. Devices meeting the 802.11a standard operate at a frequency of 5 GHz at speeds of up to 54 Mbps. Because 802.11b and 802.11a equipment operate on different frequencies, they are not compatible. Devices that meet the 802.11g standard operate at the 2.4 GHz frequency of 802.11b and the 54 Mbps speed of 802.11a; therefore, they are backwards compatible with 802.11b devices. Although all U.S. devices that meet the same standard should work together, this may not be true outside the United States.

We're Now Printer Friendly

Found an interesting article in this issue of *TechBeat* you'd like to share with someone or distribute at a meeting? Well, now you can.

Although every edition of *TechBeat* is available for online viewing in PDF and ASCII formats, you now can read and/or download printer-friendly versions of individual articles going back through 2000.

To view/download specific articles, just visit our website at www.justnet.org. Click on the blue *TechBeat* tab at the top of the home page. Then click on the issue and then the article you wish to view or print.

(Adobe® Reader® 4.0 or above required for viewing and printing.)

TechBeat ***is the award-winning newsmagazine of the National Law Enforcement and Corrections Technology Center (NLECTC) system. 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 25 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 25 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 2004 issue of *TechBeat,* published by the National Law Enforcement and Corrections Technology Center, a program of the 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; and the APEX 2001 Award of Excellence for Magazines and Newspapers–Printed.

Photo Credits: Photos used in this issue of *TechBeat* copyright © 2004 PhotoDisc, Inc.; Thinkstock; and Artville.

Staff: Managing Editor, Rick Neimiller; Writers, Becky Lewis, Jackie Siegel, and Warren Smith; Editor, Michele Coppola; Assistant Editor/Writer, Brian Higgins; Graphic Designers, C. 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.

Frequently Asked Questions

Frequently Asked Questions offers detailed information based on thousands of calls to our information specialists.

Publications

Publications from NIJ and NLECTC that you can view or download to your system.

Calendar of Events

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

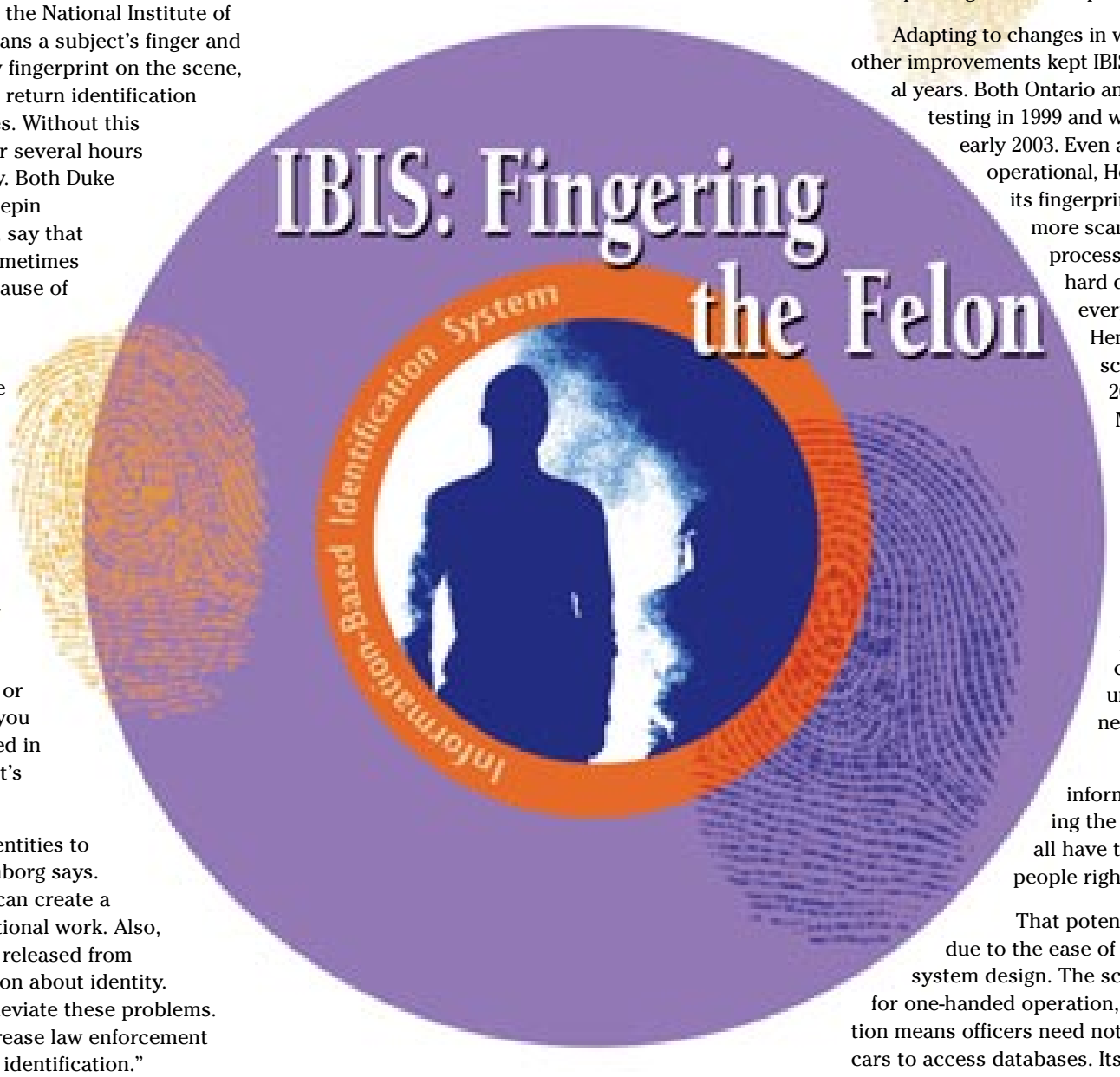
Links

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.

IBIS: Fingering the Felon

An officer stops a car for a traffic violation and asks the driver for identification. The man says he must have left his wallet at home, but his name is John Smith and he lives at 222 Any Street. The officer nods, then pulls a compact device from his belt and asks the driver if he minds undergoing a fingerprint scan. The driver, who has heard about these scanners, grudgingly extends his finger, muttering that his name is really Bob Jones and he lives at 333 Some Street.



According to Lt. Steve Duke, word about these scanners is on the street, at least in Ontario, California, where officers began using the system in 2003. During its first 6 months of operation, officers used the department's Information-Based Identification System (IBIS) [also known as Integrated Biometric Identification System] 3,737 times to identify 816 individuals and detain 164. In Hennepin County, Minnesota, during the same period, sheriff's deputies used the system 679 times, identifying 110 individuals and detaining 37.

Developed and produced by Identix Incorporated through a grant program of the National Institute of Justice (NIJ), the system scans a subject's finger and generates a forensic-quality fingerprint on the scene, then searches databases to return identification results within 2 to 3 minutes. Without this device, it can take an officer several hours to verify a subject's identity. Both Duke and Robert Hamborg, Hennepin County's program manager, say that in the past, field officers sometimes had to release subjects because of this delay.

"The longer it takes to identify a suspect, the more paranoid that person may become," says Duke, who heads the Ontario Police Department's Administration Bureau, which includes the Technology and Special Projects Unit. He might stand there thinking, 'They're trying to find out who I really am,' and decide to attack the officer or make a run for it. Anytime you can reduce the time involved in the identification process, it's a good thing."

"Suspects give false identities to officers on the street," Hamborg says. "Establishing true identity can create a substantial amount of additional work. Also, the wrong person could be released from custody because of confusion about identity. We are looking to IBIS to alleviate these problems. The technology should increase law enforcement officer safety and speed up identification."

Using a fingerprint identification system to speed up identification could prove beneficial not only to law enforcement, but also to average citizens, Duke explains. "We recently stopped a man who said he left his license at home. When the officers just ran his name, the search turned up an arrest record under his name and address. The officer asked him if he minded using IBIS, and the suspect said no, of course not. It turned out that his prints did not match those associated with the arrest record, so IBIS proved he was not that person. It turned out the man's brother had been arrested and had given his name. We were able to swear a warrant out against the brother for providing false identification information to the police."

According to Duke, Ontario gives all potential suspects—like the man mentioned above—the option of refusing to have their fingers scanned, but no one did in the first 6 months of use. If the subject agrees, he or she places a finger on the officer's small handheld scanner. The officer can also tilt the device to use a small camera to photograph the subject. Duke explains that Ontario officers use the photos when they need to identify more than one person. For example, he says, they might break up a gang fight and line everyone up on the curb. An officer starts moving down the line, scanning the first gang member's fingerprint and taking a picture. While he moves on to the second person, the system begins processing the first fingerprint. "When you get to the end, you can use the pictures to go back and say 'We have positive identification on you, and you, and you.' " Officers erase the photos and fingerprints after they complete the identification process rather than store them in a database.

The Ontario Police Department has plans for a voluntary fingerprint database (separate from the police database) that could be used to identify people with Alzheimer's disease and other kinds of dementia who are lost. If officers found a protected individual wandering the streets, they could use the system for identification and call a family member or appropriate care facility.

This represents just one potential use, Duke says. "Like everything else, technology changes constantly. Just when I think it's done, then someone thinks of more things that the IBIS could do."

"Additional funding is being used to improve the product and to keep current with evolving technology," says Joseph Cecconi, NIJ program manager for the project, originally called Squad Car Unit Identification (SQUID). Other possible improvements and applications suggested by Duke, Hamborg, and Cecconi include—

- Adding a database of latent fingerprints from local crime scenes.
- Adding a facial recognition component.
- Using a fingerprint system as a mobile booking station.
- Identifying people entering and leaving detention facilities.
- Improving internal airport security.

Adapting to changes in wireless technology and other improvements kept IBIS in development for several years. Both Ontario and Hennepin County began testing in 1999 and went fully operational in early 2003. Even after its system became operational, Hennepin County upgraded its fingerprint database and received more scanners. Hamborg says the process had glitches, including a hard drive failure. However, everything worked out and Hennepin County distributed scanners to an additional 20 partner agencies in the Minneapolis–St. Paul area. Hennepin County shares its fingerprint scanners with patrol officers at 25 local law enforcement agencies, the Minnesota Bureau of Criminal Apprehension, and the Bloomington police at the Mall of America. Ontario also shares its units with a number of neighboring jurisdictions.

"We already were sharing information, and now, by sharing the fingerprint scanners, we all have the potential to identify people right on the spot," Duke says.

That potential exists at least in part due to the ease of use incorporated into the system design. The scanner's pistol grip allows for one-handed operation, and its wireless connection means officers need not return to their squad cars to access databases. Its design makes it usable by officers mounted on horseback, bicycle, or motorcycle, and its weight of less than 2.5 pounds includes the battery pack, which allows for 3 hours of continuous operation and 14 hours of standby operation. Duke says learning to use IBIS takes only 2 to 3 hours, and his officers like that it does not compromise their ability to defend themselves.

Because of that ease of use as well as other factors, Cecconi says NIJ hopes that this program "will result in more widespread use by law enforcement agencies throughout the country." Its present cost and durability might make it prohibitive for some law enforcement agencies, but that could change with future versions.

For more information on the IBIS program, contact Joe Cecconi, 202–305–7959 or cecconij@ojp.usdoj.gov; Lt. Steve Duke, 909–395–2711 or sduke@ontariopolice.org; or Robert Hamborg, 763–525–6203 or Robert.Hamborg@co.hennepin.mn.us.

the NLECTC 'center system'

The National Law Enforcement and Corrections Technology Center (NLECTC) system, a program of the 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 deliver information and technology assistance to 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 has been able to deliver expertise in a number of technologies by forming partnerships with such host organizations as the Air Force Research Laboratory, the Space and Naval Warfare Systems Center, and The Aerospace Corporation. Through these partnerships, NLECTC staff have access to the latest innovations in research and development.

The NLECTC system serves as an "honest broker" resource for technology information, assistance, and expertise.

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 excess and surplus 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 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 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 also has 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), Operation America (bomb detection technologies), 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

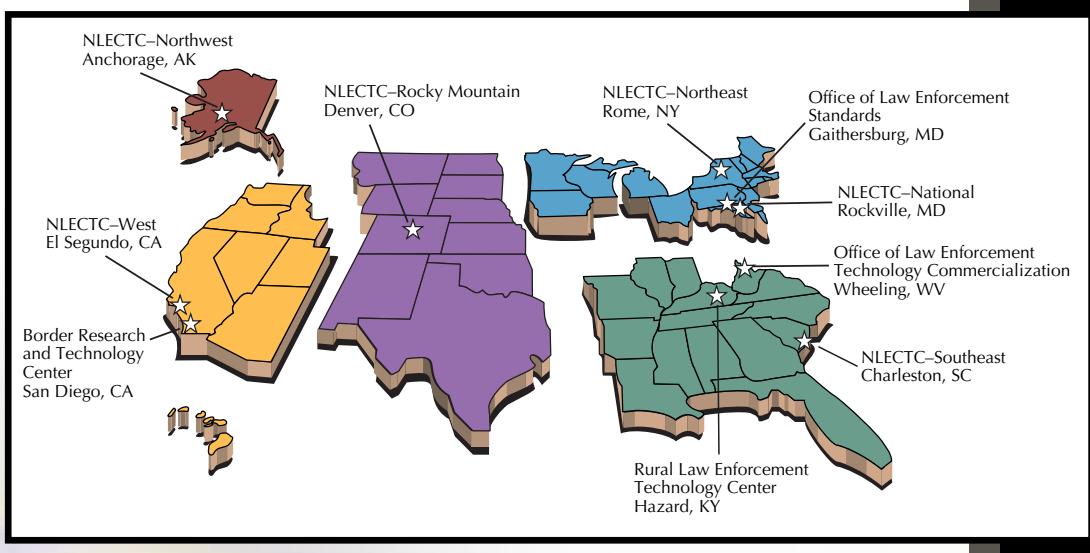
NLECTC disseminates information to the criminal justice community at no cost through educational bulletins, equipment performance reports, guides, consumer product lists, news summaries, meeting/conference reports, videotapes, and CD–ROMs. NLECTC also publishes *TechBeat,* an award-winning quarterly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

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.

Technology Needs Assessment

Our national body of criminal justice professionals—the Law Enforcement and Corrections Technology Advisory Council (LECTAC)—ensures that we are focusing on the real-world needs of public safety agencies.



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 co-located with or supported by federally funded technology partners so they can leverage unique science and engineering expertise.

NLECTC–National
2277 Research Boulevard
Rockville, MD 20850
800–248–2742
asknlectc@nlectc.org

NLECTC–Northeast
26 Electronic Parkway
Rome, NY 13441–4514
888–338–0584
nlectc_ne@rl.af.mil

NLECTC–Southeast
5300 International Boulevard
North Charleston, SC 29418
800–292–4385
nlectc-se@nlectc-se.org

NLECTC–Rocky Mountain
2050 East Iliff Avenue
Denver, CO 80208
800–416–8086
nlectc@du.edu

NLECTC–West
c/o The Aerospace Corporation
2350 East El Segundo Boulevard
El Segundo, CA 90245–4691
888–548–1618
nlectc@law-west.org

NLECTC–Northwest
3000 C Street, Suite 304
Anchorage, AK 99503–3975
866–569–2969
nlectc_nw@ctsc.net

Border Research and Technology Center (BRTC)
1010 Second Avenue, Suite 1920
San Diego, CA 92101–4912
888–656–2782
info@brtc.nlectc.org

Rural Law Enforcement Technology Center (RULETC)
101 Bulldog Lane
Hazard, KY 41701
866–787–2553
ruletc@aol.com

Office of Law Enforcement Technology Commercialization (OLETC)
2001 Main Street, Suite 500
Wheeling, WV 26003
888–306–5382
oletc@oletc.org

Office of Law Enforcement Standards (OLES)
100 Bureau Drive, Stop 8102
Gaithersburg, MD 20899–8102
301–975–2757
oles@nist.gov

TECH SHORTS

Technology News Summary

TechShorts is a sampling of article abstracts published weekly as part of the National Law Enforcement and Corrections Technology Center's (NLECTC's) online information service: the *Law Enforcement and Corrections Technology News Summary.*

Offered through JUSTNET, the website of NLECTC, this weekly news summary provides synopses of recent articles relating to technology developments and initiatives in law enforcement, corrections, and the forensic sciences that have appeared in newspapers, newsmagazines, and trade and professional journals. The summaries also are available through an electronic e-mail list, *JUSTNETNews.* Each week, subscribers to *JUSTNETNews* receive the summary directly via e-mail.

To subscribe to the *JUSTNETNews/Law Enforcement and Corrections Technology News Summary,* e-mail your request to asknlectc@nlectc.org or call 800–248–2742.

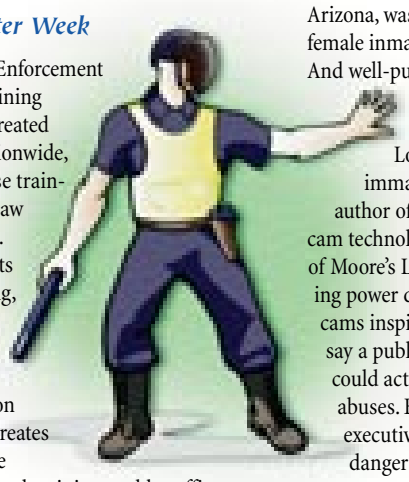
Navy Brig Testing Biometric Tracking

Associated Press

The National Institute of Justice (NIJ) has partnered with the Navy's Consolidated Brig to test biometric tracking technology that replaces paper documentation for recording prisoners' movements at the Consolidated Brig, which holds a number of terrorist suspects. The monitors will track prisoners through finger- and hand-identification scans. Testing will be limited to only those prisoners held as terrorist suspects in the facility's high-security area. Project developers considered a number of identification technologies before choosing finger- and hand-identification scans. Nineteen monitors are installed in the brig to track the movements of terrorist suspects and scan the fingers and hands of the prisoners. NIJ researcher Allan Turner says the next logical step is to deploy the technology in a State prison. For more information, log on to http://www.thestate.com/mld/thestate/news/local/7387587.htm.

Putting a Little SWAT in Every Cop

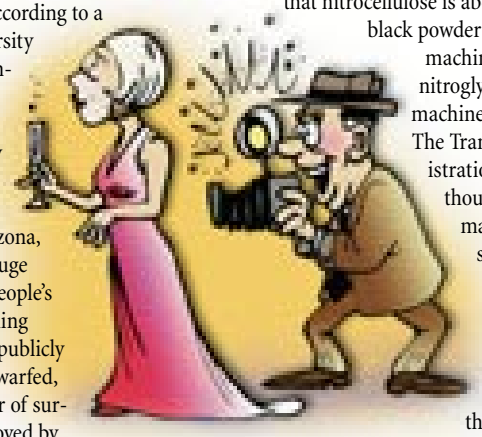
Federal Computer Week



The Advanced Law Enforcement Rapid Response Training (ALERRT) Center, created in 2002, offers a nationwide, cost-effective, intense training program for all law enforcement groups. The program consists of classroom training, mock exercises employing paintball-style weapons, and interactive simulation technology that re-creates several risky real-life situations. Video-based training enables officers to practice in a hands-on atmosphere in situations they may have experienced and ultimately offers a measurement tool to determine their judgment in such scenarios, according to center officials. ALERRT has so far instructed around 750 officials in Texas, where the center is headquartered, in the past year. The center has three operational high-tech firing ranges on its almost 200-acre locale, although it does not have a central building for classes, exercises, and training. Instructors have instead been traveling to schools and additional public facilities across Texas. Although the center has obtained a $485,000 grant from the Department of Justice, it is pursuing $6 million to construct a new training facility. A longer term objective is to establish a "train-the-trainer" program, a 2-week endeavor that would permit the center to instruct officers from around the United States so they, in turn, can instruct their colleagues. For more information, log on to www.fcw.com/fcw/articles/2003/0922/tec-swat-09-22-03.asp.

We Are All Paparazzi Now

Salon.com



Publicly accessible webcams are proliferating throughout the world with more than 10,000 webcams worldwide, according to a Carnegie Mellon University survey this past September. Paul Lancaster, an Arizona businessman who operates a publicly accessible webcam focused on Heritage Square in Flagstaff, Arizona, says webcams attract huge audiences because of people's innate interest in watching others. The number of publicly available webcams is dwarfed, however, by the number of surveillance cameras deployed by private and government entities nationwide—more than 3 million cameras, according to the Security Industry Association. Existing wiretap laws make secretly recording public conversation illegal, but no laws protect people's images recorded in public places. But recently, a county sheriff in Phoenix, Arizona, was ordered to stop webcasting images of female inmates for commercial use via "jailcams." And well-publicized facial recognition systems used by the Tampa Police Department for the 2001 Super Bowl and in Boston's Logan Airport have failed because of immature technology. However, David Brin, author of *The Transparent Society* warns that webcam technology will continue to improve at the pace of Moore's Law, which states that computer processing power doubles every 18 months. Although webcams inspire "Big Brother" fears, some observers say a public, distributed network of webcams could actually prevent government civil liberty abuses. Electronic Privacy Information Center executive director Marc Rotenberg says the real danger of webcam networks, especially in the government sphere, is the physical infrastructure, which cannot be removed as easily as privacy-infringing legislation. For more information, log on to www.salon.com/tech/feature/2003/09/25/webcams/index.html.

Pillow Bombs Feared on Planes

Washington Post

Al Qaeda operatives have been trained to create a special cotton-like type of explosive that can be placed inside coats, stuffed animals, and pillows aboard U.S. airliners, according to U.S. intelligence officials. The Homeland Security Department circulated a warning about the potential explosives to airlines and airport security officials in early August 2003. The explosives are created by mixing nitric acid or sulfuric acid with cotton or a cotton-like substance and then adding nitroglycerine. The resulting substance, known as nitrocellulose, can be packed tightly into a container or other space and then lit to create an explosion of some significance. Gregory Baur, former director of the International Association of Bomb Technicians and Investigators, says that nitrocellulose is about as combustible as the black powder used in ammunition. X-ray machines are incapable of detecting nitroglycerine, but trace-detection machines can detect the substance. The Transportation Security Administration (TSA) has bought thousands of trace-detection machines in preparation for such a scenario. In fact, for several years now, the TSA has been anticipating the threat of explosives hidden in toys and clothing, and has taken steps to address this potential threat, says a TSA spokesman. For more information, log on to www.washingtonpost.com/wp-dyn/articles/A21509-2003Oct13.html.

'Dog-on-a-Chip' Could Replace Drug-Sniffing Canines

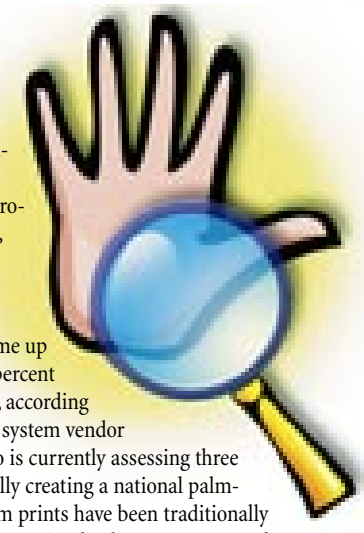
AScribe Newswire

Researchers at the Georgia Institute of Technology have developed a chip that allows law enforcement to detect illegal drugs via a handheld device. Dogs are currently employed in this capacity, but have difficulty distinguishing odors of illicit drugs from other substances, and they need trainers to oversee them. Georgia Tech researcher William Hunt says the chip's design is based on two types of technology: Microelectronics and biotechnology. The chip uses surface acoustic wave electronics to detect the presence of illicit chemicals via sound waves, plus monoclonal antibodies to detect chemicals through molecular interactions. Hunt notes the technology is the first of its kind to employ cloned copies of proteins. The technology offers cost and time advantages over using dogs for drug detection. The chip performed successfully during a field test with the Georgia Bureau of Investigation. Results of the study will be published in the American Chemical Society's Analytical Chemistry journal.

Elementary, Watson: Scan a Palm, Find a Clue

New York Times

Because many of the prints found at crime scenes are from suspects' palms rather than their fingers, the New York Police Department in 2003 began having prisoners place their entire hands over the scanner that captures their palm prints, rather than just their fingerprints. The department has collected 100,000 palm prints so far, and next month it will be able to do computerized matches of the prints in this database. So far, about 30 law enforcement agencies around the country have built their own palm databases, including the Los Angeles Metropolitan Area, Miami, Palm Beach, Philadelphia, and Indianapolis. Thus far, Indianapolis has come up with a match in 15 percent of its palm searches, according to statistics from its system vendor Identix. The FBI also is currently assessing three systems for potentially creating a national palm-print repository. Palm prints have been traditionally taken by ink, but palm-print databases are expected to increase matches exponentially. The Manhattan police academy has installed ILS2 palm scanners that walk officers through the print collection process and alert them of bad prints. The New York Police Department will be one of the first to use an inkless scanner to record prints directly into the database, notes James Simon of the NYPD's Central Records Division.



Nanoparticles Clearly Finger the Culprit

New Scientist

Researchers at the University of Sunderland in England are developing oil-seeking nanoparticles that could one day supplant the fluorescent power used currently in detecting fingerprints. The tiny glass particles are speckled with a fluorescent dye and coated with hydrophobic molecules, which are repelled by water and attracted to oil. Current fluorescent power sticks to oily residue left by a fingertip, but lifted prints sometimes lack clarity. The nanoparticles, according to the researchers, should pick out even the faintest prints. For more information, log on to www.newscientist.com/news/news.jsp?id=ns99994348.

Cops, Residents Chat It Up Via Net Link

San Francisco Chronicle

The police substation in North Oakland, California, has established an Internet chat room where local residents can communicate criminal incidents to police. The chat room allows the police "to provide real-time information and develop a relationship with residents and communicate with community leaders," says Oakland police Lt. Lawrence Green, who created and launched the chat room in June 2002. The chat room currently has more than 235 community members, including Oakland officials and police officers. The chat room has proved to be so popular and effective that Oakland Police Chief Richard Word has decided that all the city's police substations must create similar chat rooms. Five additional chat rooms have been launched since March of 2003. Should these types of chat rooms be established in other U.S. cities, they could prove to be an excellent tool for integrating the viewpoints and observations of residents into police departments' "focused enforcement" plans. For more information, log on to http://www.sfgate.com/cgibin/article.cgi?file=/chronicle/archive/2003/11/28/CCGTB3A45D1.DTL&type=tech.

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 offsite conference support, and other technical assistance. The easiest way to access NCJRS is online.

Start at http://www.ncjrs.org. 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 and calendar of events databases.

Stay informed. Register at *http://puborder.ncjrs.org/register* to receive—

- ***NCJRS Catalog.*** A bimonthly periodical that highlights recent publications and products and contains a convenient online order form.
- ***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.

Ask questions. Share comments. Get answers to your questions or share suggestions about NCJRS services at—

- *http://askncjrs.ncjrs.org* (questions)
- *http://tellncjrs.ncjrs.org* (comments)

NCJRS Contact Information at a Glance

Web: *http://www.ncjrs.org*

Phone: 800–851–3420
(Monday – Friday,
8:30 a.m. to 7 p.m. e.s.t.)

Fax: 301–519–5212
(requests for assistance)
410–792–4358
(publication orders)

Mail: NCJRS, P.O. Box 6000,
Rockville, MD 20849–5000

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #96–MU–MU–K011 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 Aspen Systems Corporation. 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.

NIJ Technology Institutes 2004

Law Enforcement Technology Institute
July 11–16, 2004
Application Deadline: June 1, 2004

Corrections

Law Enforcement

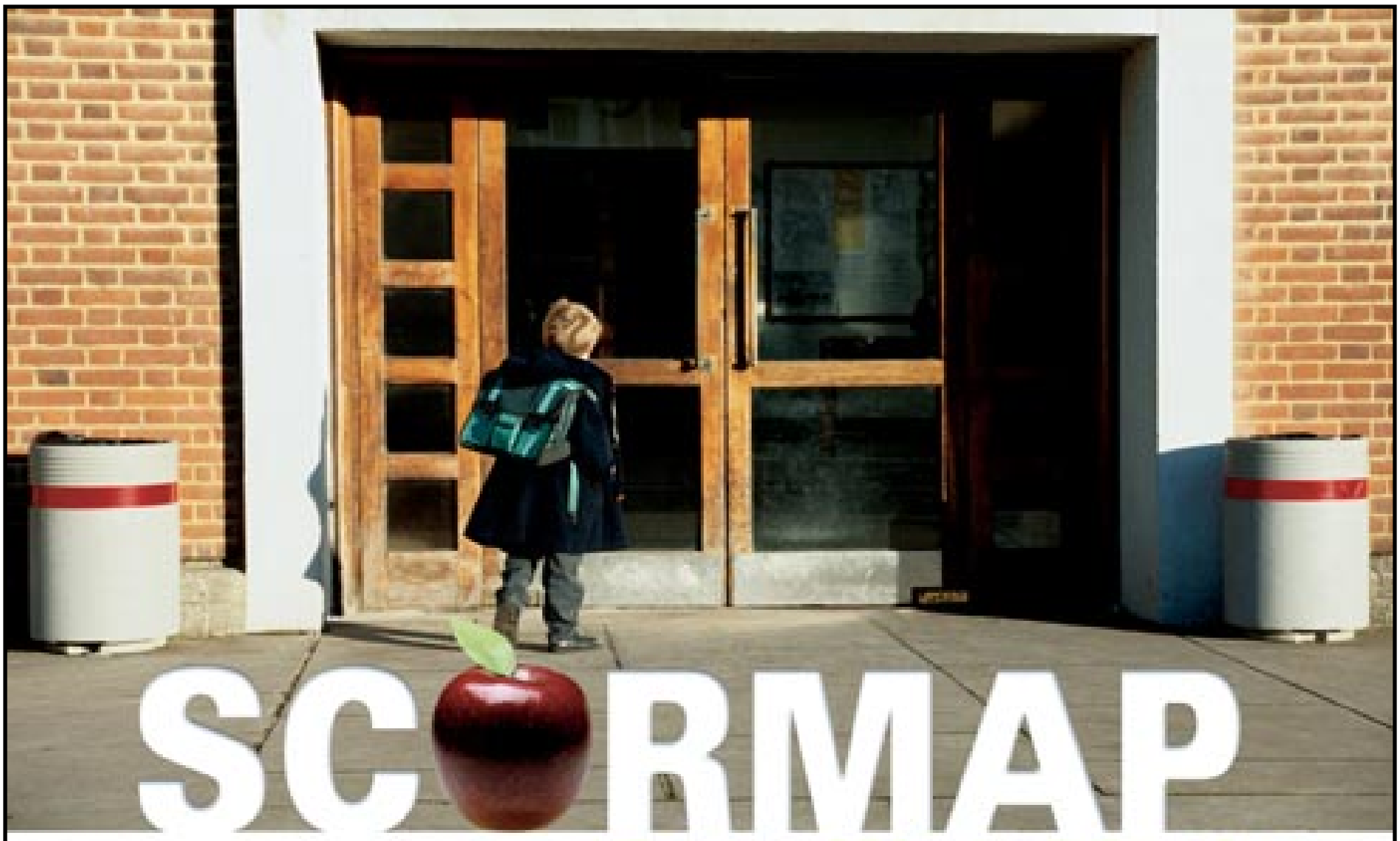
Corrections Technology Institute
September 19–24, 2004
Application Deadline: July 30, 2004

For more than 5 years, the National Institute of Justice (NIJ) has sponsored two annual Technology Institutes—one specifically for law enforcement personnel; the other for corrections personnel.

Both Technology Institutes are held in Washington, D.C., and run for 5 days, during which participants receive information and assistance on existing and developing technologies, work through problems relating to technology implementation, and exchange technology lessons learned of importance to law enforcement or corrections. In addition, those attending receive briefings and demonstrations at various agencies and departments in the metropolitan area.

Participants from across the country bring to the Institute questions, technology problems and solutions, and a desire to do their jobs more efficiently and effectively.

There is no cost for either Institute, and all travel, food, and lodging expenses are covered. However, only 25 to 30 individuals are selected to attend (no previous attendees, please). Applications and additional information for both Technology Institutes are available online at www.justnet.org or by calling 800–248–2742.



SCORMAP Gets High Marks

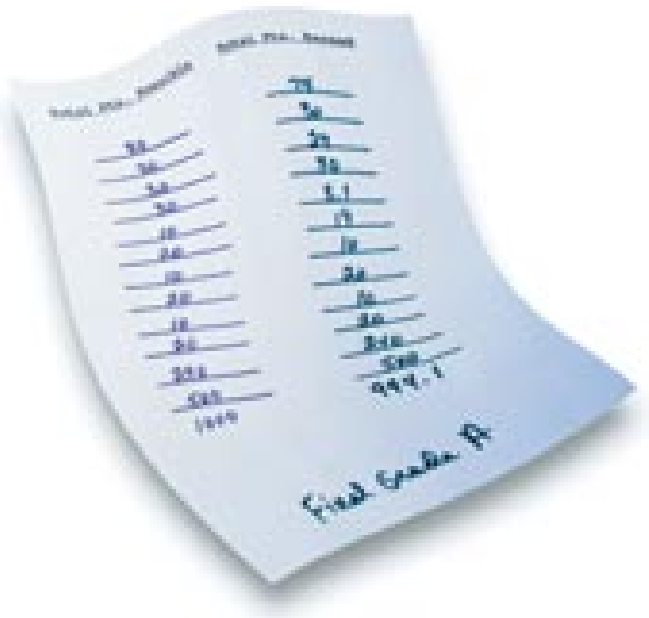
The beep-beep of an emergency broadcast sounds on the radio . . . a funnel cloud has been spotted. Pleasant Valley Elementary School, in Calhoun County, Alabama, at once implements its severe weather plan. Administrators turn to a nearby computer and access vital information stored in the school's SCORMAP program—information about student attendance, emergency exits, and utility shutoffs.

Although this scenario remains hypothetical, Pleasant Valley Elementary and other schools in Calhoun County have become the Nation's test bed for SCORMAP, a mapping software program that uses Geographic Information Systems (GIS) and Computer Assisted Drawing (CAD) technologies to put detailed information at school administrators' fingertips. Its objective is not only to promote school safety but to help administrators, school resource officers, and local law enforcement in emergencies.

SCORMAP is based on CORMAP, an application for correctional facilities developed in 1999 by the National Institute of Justice's National Law Enforcement and Corrections Technology Center (NLECTC)–Southeast and the U.S. Department of Energy's Savannah River Technology Center (SRTC). Until recently, a major hurdle to mapping multistory buildings such as prisons or schools was the duplicate, room-above-room construction, which GIS could not map alone. In cooperation with SRTC, NLECTC–Southeast overcame this problem by integrating CAD and GIS technologies. Now, multilevel areas can be displayed in a three-dimensional layout. Each room (or cell) on each floor becomes a separate, identifiable unit that can be displayed on a computer screen.

According to Lisa Russell, information technology director for Calhoun County Schools, school mapping began early last fall, but it will take several years to map every school in the county. With almost 20 schools in the system, Pleasant Valley Elementary School was chosen as the starting point because this small new school already had some of the necessary information digitized.

Rob Donlin, project manager for corrections and school safety at NLECTC–Southeast, says



SCORMAP has the capability to store any information school administrators think they may need. "We map physical aspects, but we also track student characteristics," Donlin says. "If a child turns up missing, the system can help track him down by showing, for example, that he didn't get on the bus to go home."

Information stored in SCORMAP includes fire evacuation routes, severe weather holding areas, water and electrical shutoffs, air conditioning and heating shutoffs, breaker boxes, and fire extinguishers. Russell says that she knows access to this information in an emergency could prove vital to Calhoun County's school resource officers and local law enforcement.

Calhoun County Sheriff Larry Amerson got the SCORMAP project rolling by introducing Russell to Donlin. "Sheriff Amerson knew about CORMAP because Rob Donlin helped him map the local jail. He knew we were forward thinking, and he put us together," Russell explains. Donlin met with Russell and Calhoun County's Safety and Security Director Mike Fincher in fall 2002. They agreed to start when the next school year began.

"Because the school system's funds for this type of project are limited, we were very glad to receive technology assistance from NLECTC–Southeast," Russell says. "All in all, this is a good partnership. Rob Donlin and his team have been helpful as a general school safety resource in addition to helping with the mapping." NLECTC–Southeast helped Fincher attend a national conference on campus safety, and he came back with more ideas for improving safety in Calhoun County schools.

"This kind of partnership bleeds over into a lot of other opportunities," Russell says. "Even though it will take several years to put [SCORMAP] completely into place, we couldn't have done it on our own, because we don't have the resources."

Donlin says CORMAP required a few modifications to morph into SCORMAP, for the most part adding passwords so that only authorized personnel could access such student-specific information as medical records. Also, although CORMAP used inmates' assigned beds as their "location address," SCORMAP uses desks for elementary school students and lockers for secondary school students.

For more information on SCORMAP and CORMAP projects, contact Rob Donlin at the National Law Enforcement and Corrections Technology Center–Southeast, 800–292–4385 or donlin@nlectc-se.org. For information on Calhoun County Schools' experience with SCORMAP, contact Lisa Russell, 256–741–7475 or lrussell@calhoun.k12.al.us.

"The days of going out and measuring skidmarks and using calculus to determine speed are over."

(Scene of the Crash . . . cont. from page 1)

The course, Mael says, covers three basic areas:

- Mapping technology, including tools that capture data on the scene, and computer-aided drafting or mapping software that diagrams the scene. "We actually go outside and do a mock scene," says Mael. "Then participants have to create a usable map."
- Black box technology, including a field trip to a salvage yard to extract data from a black box onboard a wrecked vehicle. Depending on the manufacturer, the black box yields such information as how many people were in the car, how fast it was going on impact, and whether or not the seatbelts were buckled.
- Reconstruction management and calculation software that performs the calculations and analysis of field data. Mael says that one of the CAD programs that is demonstrated has the capacity to do the velocity equations as you do diagrams.

In the past, low-tech tools such as measuring tapes and scratch pads led to less-than-accurate results, Krenning notes. Today, a point-and-shoot laser rangefinder about the size of a radar gun can measure distances to within one-tenth of an inch and then download the data into a handheld unit similar to a personal digital assistant. With proper training, a single officer can diagram and chart an entire scene in a fraction of the time it would have taken a team of investigators using manual methods. The techniques also can be applied to other types of crime scenes.

This year, NLECTC–Rocky Mountain is offering the course throughout its 10-State region that includes Colorado, Kansas, Montana, Nebraska, New Mexico, North and South Dakota, Oklahoma, Texas, and Wyoming. In addition, courses geared toward prosecutors are in development.

For more information about "Crash Scenes Technologies," including scheduling, contact Troy Krenning at NLECTC–Rocky Mountain, 800–416–8086, 303–871–4369, or tkrennin@du.edu.

National Law Enforcement and Corrections Technology Center
2277 Research Boulevard
Mail Stop 8J
Rockville, MD 20850

PRESORTED STANDARD
U.S. POSTAGE PAID
ANNAPOLIS JUNCTION, MD
PERMIT NO. 2538