I t is considered the ultimate in recycling and has proved to be nothing short of a financial windfall for law enforcement and corrections agencies.

Although in existence for more than a decade, this group of programs was unknown to most police and corrections agencies until the National Institute of Justice’s (NIJ’s) National Law Enforcement and Corrections Technology Center (NLECTC–Southeast) stepped in. Beginning in the late 1990s, NLECTC–Southeast initiated training and support efforts to put equipment into the hands of the Nation’s police and corrections officers through—

■ The 1033 Program.
■ The Defense Automation Resources Management Program.
■ The 1122 Program.

NLECTC–Southeast’s Ken Dover, who trains police and corrections personnel to take advantage of these four programs, says a number of State and local law enforcement agencies have even built or augmented their air operations using property obtained through the programs. They use the airplanes and helicopters for drug interdiction, marijuana eradication, manhunts, and search-and-rescue missions. The cost of the aircraft to the agencies is minimal—just the expense of getting the equipment to its destination.

These rather substantial “donations” from the Federal Government are deemed excess property and made available to public safety agencies. Dover says. Airplanes and the like are not the only equipment available. The Federal Government’s inventory includes various types of aircraft, armored personnel carriers, 18-wheelers, pickup trucks, engines and parts, computers, toolboxes and tools, night vision equipment, binoculars, rifles, shotguns, canyons, cots, radios, backpacks, tents, utility uniforms, boots, helmets, gas masks, and more.

The 1033 Program

The 1033 Program began in 1989 as the 1208 Program. It made surplus U.S. Department of Defense (DoD) equipment available to law enforcement for use in counterdrug activity. In 1996, the program was opened to all law enforcement activities, with special consideration given to agencies that wanted equipment for counterdrug or counterterrorism activities.

The 1033 Program is administered at the State level by a coordinator. Some coordinators work alone while others have a full-time staff. These staffing differences can produce dramatically different results. One State with a dedicated staff brought in more than $20 million in Federal surplus property in 1 year. Another State, which assigned a full-time police officer to handle the coordinator task in his spare time, brought in only $1.5 million in equipment.

Dover says DoD makes a distinction between “excess” and “surplus” property. Excess property is equipment that has been shipped to a Defense Reutilization and Marketing Office (DRMO) and has been in stock for less than 21 days. After that period, anything not “tagged” by a Federal, State, or municipal law enforcement or corrections agency is considered surplus. This equipment is then made available to other agencies, such as fire departments, schools, hospitals, or organizations that support the activity of State, county, or local governments. Although there is no charge for excess or surplus property, some States impose a handling fee (generally 1 to 20 percent of an item’s original cost). All items are made available “as is” and “where is.”

The acquiring agency is responsible for making transportation arrangements.

NLECTC acts as the liaison between DoD, the Defense Logistics Agency; the Law Enforcement Support Office, which operates the program; and the law enforcement and corrections communities. NLECTC advises and supports the 1033 Program’s State coordinators, teaching them about the program, helping them with paperwork, and supporting them as they try to improve their individual systems.

The Check Is in the Mail

ll and elderly individuals confined to their homes or beds look forward to the postman’s daily delivery, hoping their day might be brightened by the arrival of a card, a letter from a friend, or a package. Individuals confined to correctional facilities also anticipate the mail’s arrival, but they may be hoping for something other than a friendly greeting: hidden drugs.

For correctional facilities, stopping drug contraband in the mail is a full-time job. With funding from the National Institute of Justice (NIJ), the U.S. Department of Defense (DoD) Counterdrug Technology Development Program Office (COTDPO) is conducting a study to identify technologies that would simplify the task.

“Our goal is to find a device and process to screen mail and packages for drugs,” says Dr. Allan Turner, visiting scientist at NIJ’s Office of Science and Technology.

“Inmates and others try to introduce drugs through packages, letters, magazines—you name it,” Turner adds. “The most recent 1033 Program improvement is the ability to tag equipment online. You’ve always been able to look at available equipment online,” Dover says, “but to tag it for yourself, you had to fax handwriting paperwork back and forth. Earlier this year the Law Enforcement Support Office started a program in four States to tag equipment online, with the goal of having online tagging in place nationwide sometime this summer.”

Dover says a current goal is to expand the use of the program by law enforcement and corrections and encourage these agencies to work together to acquire equipment. “The 1033 Program’s customer base has about 8,000 active State law enforcement agencies and 500 Federal agencies. That’s not much when you realize there are 19,000 law enforcement agencies in this country. Some don’t know about the program and some aren’t able to participate because of their size, location, or lack of support. What we’d like to do is get [See Surplus Property, page 2]
them to band together to take advantage of excess Federal equipment at no or very low cost.”

**Defense Automation Resources Management Program Management**

The Defense Automation Resources Management Program (DARM) is one of the oldest Federal programs that handles excess equipment. The program, operated by the Defense Information Systems Agency (DISA), differs from the 1033 Program in two ways. First, it focuses exclusively on information technology, making available everything from mainframes and personal computers to monitors, scanners, and printers. Second, whereas the 1033 Program sends equipment to one of its DRMOs for screening and distribution, DISA cuts out the middleman and allows State coordinators to tag items online.

“However, there’s no preview, no picture, and you can’t go see the equipment like you can at a DRMO,” says Sharon Sellers, Defense Special Programs Chief. “What you can do is call the current owner to discuss its technical capabilities.”

Sellers says that under the program, DoD agencies, their contractors, and other government agencies have first option on available equipment. Anything that has not been tagged after 15 days becomes available to law enforcement. As in the 1033 Program, the receiving agency is responsible for shipping costs and the State coordinator may levy a fee on the items obtained. In late 2001, DISA automated its 20-year-old paper process. In the past, agencies that wanted equipment submitted a request form and waited an average of 3 to 5 days for approval. Now, property managers and State coordinators can electronically request a hold on equipment they want and have their requests approved online by the DARM staff within 1 to 2 business days.

**1122 Program**

The 1122 Program allows State and local governments to purchase new equipment at a reduced cost. They will pay a fee, and the receiving agency is responsible for shipping costs and the State coordinator may levy a fee on the items obtained. In late 2001, DISA automated its 20-year-old paper process. In the past, agencies that wanted equipment submitted a request form and waited an average of 3 to 5 days for approval. Now, property managers and State coordinators can electronically request a hold on equipment they want and have their requests approved online by the DARM staff within 1 to 2 business days.

**Night Vision Systems Law Enforcement Support Program**

Night vision equipment is expensive. If you need to repair or replace your equipment, it can cost hundreds of thousands of dollars, and repair costs may run as high as the original investment.

The Night Vision Systems Law Enforcement Support Program provides night vision devices costing more than $4,000 on the commercial market for a fee of $300 per unit, per year, through a loan-lease arrangement. Sponsored by the Naval Surface Warfare Center in Crane, Indiana, the Night Vision Systems Law Enforcement Support Program puts high-quality night vision goggles (model AN/PVS-5) that have been refurbished to military standards into the hands of large and small agencies. The $300 fee covers refurbishing and administrative costs.

Should the goggles need to be repaired at any time, the center will ship a replacement at no additional cost, resulting in minimum downtime for an agency. As new versions of the goggles become available, the center replaces the AN/PVS-5s with an upgraded model, also at no additional cost. The center includes in its program the repair of agency-owned night vision and thermal imaging equipment at actual repair costs. In the future, the center plans to extend the program to include light-intensifying, handheld night vision scopes and pocket scopes.

**Defense Logistics Agency. Items available include aircraft fuel, lubricants, oils, and greases; and all types of new and used aircraft tires; rope (wire and fibrous) and tie-down straps; roof bar mounts; safety harnesses; locks and seals; telephone and power cables; cameras, accessories, and film; binoculars; dry batteries; cameras, accessories, and film; binoculars; dry batteries; camera slide; and various emergency response and supplies—in addition to 80 laptop computers—to various emergency response and supply agencies.**
name it, they try to slip drugs in it. The process of finding drugs is very
labour intensive. We’re looking for a way for technology to make it easier and
better.”

To determine which products might meet its criteria, DoD started with a
survey to locate products already on the market, then moved into a three-
step research process. The first step involved simply testing to see “how
well the technologies found drugs, period,” says Duane Blackburn, deputy
program manager at COTDPO. This led to the discovery that ion spectrome-
try scanners could find mere nanograms of drugs. To visualize a nanogram,
Blackburn says, consider a paperclip, which weighs approximately 1 gram.
Divide it into 1 million pieces. Divide 1 of those pieces into 1,000 pieces.
That would be a nanogram.

For the second step, a scenario evaluation, DoD set up a mock prison
mailroom at the Thunder Mountain Evaluation Center in Fort Huachuca,
Arizona. Thunder Mountain, established to test methods of detecting large
amounts of drugs coming through U.S. Customs, provided the clean rooms
and experience needed to create the mock mailroom.

Before testing began inside the mock mailroom, DoD set out to deter-
mine whether mail picks up trace contamination just in making its way
through the U.S. Postal Service. “Keep in mind that even a clean envelope
that you just bought at Walmart could test positive for minute traces of
chemicals that could be drugs,” Blackburn says. Researchers sent a test
mailing from a local post office and another mailing from across the country
and compared the results with a control batch. They found no increase in
trace contamination due to an envelope simply being mailed.

Next, they “spiked” test mail with drugs (this batch always remained in
the mock mailroom) to find out how well the various products located the
contaminated letters. In addition to the scanners, DoD also tested x-rays
and Mistral sprays, which change color in the presence of drugs. The last
two products did not detect the presence of drugs in the small quantities
typically smuggled through a penitentiary mailroom.

So far, research has yielded encouraging results for two commercially
available ion mobility spectrometry scanners (one handheld and one desk-
top). Concern remains, however, about the possibility of too many false posi-
tive readings caused by trace amounts of drugs, and additional testing may
be needed. Blackburn says that both vendors’ scanners can detect the pres-
ence of drugs in nanogram amounts. Sometimes, however, that may be too
sensitive. For example, money in any major metropolitan area with a
widespread drug problem is likely to test positive.

Final analysis of the research may indicate that the next step is to set
up a field test of the ion mobility spectrometry scanners in a correctional
facility, but the analysis also might recommend that researchers turn their
attention to other, more expensive technologies, such as mass spectroscopy,
which also has shown promise in detecting chemical and biological agents.

“Once we get all the results back,” Blackburn says, “we have a decision
to make. Can we come up with procedures to test the technology in an oper-
atinal evaluation, or should we test other, more expensive technologies?”
Blackburn adds that DoD began with products that use technology initially
developed 10 to 15 years ago, which puts them within the economic reach
of most correctional systems. Some correctional systems already use these
products to search their mail for drugs.

If the completed research identifies a feasible existing product, it will be
a real asset for correctional systems that now dedicate substantial staff time
to searches for drugs. For example, at the U.S. Penitentiary in Leavenworth,
Kansas, mail goes through two rounds of x-ray checks plus a hand check.
Blackburn, who spent a day observing Leavenworth’s process, says the con-
traband detection process starts with Leavenworth staff picking the mail up
at the post office instead of taking delivery. At the penitentiary, two x-ray
checks are conducted to find concealed weapons and large amounts of
drugs, while the hand search attempts to locate small amounts of drugs
sent by those trying to be clever in avoiding detection.

“Stuff working in a mailroom open each and every piece of mail and
search it,” Turner says. “Some of the methods used to slip drugs in are very
sophisticated. They’ll hide it in the folds of a newspaper, in the pages of a
magazine. Sometimes the drugs are inside the seams of a standard
envelope.”

Staff also search under stamps and address labels, and inside books and
greeting cards. They look for, and find, almost every type of drug sold on the
street: cocaine, heroin, methamphetamines, and more. While the amounts
found may seem small to agencies that enforce drug laws in the general pub-
lic, they are large enough to provide income, power, and control when in the
hands of inmates.

“Drugs in prisons and jails are a big problem,” Turner says. “You’d be
astounded at the number of people arrested who have used drugs within 30
days prior to their arrest. Common sense will tell you that if you take these
people and put them in a correctional system, they will try to get drugs. If
there’s a market, there will be sales. For a product to be useful in helping to
cut off the potential for such sales, it needs to be inexpensive, reliable, and
easy to install and use. Further research will confirm if DoD has found it.”

For more information on the Identification, Demonstration,
and Assessment of Drug Detection Technology study, contact Allan
Turner, 202–616–3509, e-mail turnera@ojp.usdoj.gov; or Duane
Blackburn, 202–365–8774, e-mail BlackburnDM@nswc.navy.mil.
Individual Subscriptions: TechBeat is available at no cost. If you are not currently on our mailing list or need to change your mailing label information, please call us at 800–248–2742 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 newsletter and we will send copies directly to them. Contact Rick Neimiller, TechBeat managing editor, at 800–248–2742, for additional information or to subscribe.

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 Summer 2002 issue of TechBeat, published by the National Law Enforcement and Corrections Technology Center, a program of the National Institute of Justice, 800–248–2742.”

Questions/Comments/Story Ideas: We welcome all questions, comments, and story ideas. Please contact Rick Neimiller, TechBeat managing editor, at 800–248–2742 or e-mail rneimiller@nlectc.org.

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 © Digital Vision; PhotoDisc, Inc.; Corbis Images; Comstock Images; Corel Corporation; Eyewire; ImageState; the National Law Enforcement and Corrections Technology Center—Northeast; and Art Explosion.

TechBeat is the award-winning flagship publication of the National Law Enforcement and Corrections Technology Center (NLECTC) system. Our goal is to keep you up to date with technologies currently being developed by the NLECTC system, as well as other research and development efforts within the Federal Government and private industry. TechBeat is published four times a year. Managing Editor, Rick Neimiller; Contributing Editor/Writer, Lois Pilant; Contributing Writers, Becky Lewis and Jackie Siegel; Editor, Michele Coppola; Graphic Designers, C. Denise Collins and Tina Kramer.
seemingly random fight between two inmates in a prison yard quickly escalates into a brawl. After corrections officers quell the disturbance and return the inmates to their cells, an incident report is filled out. On the back of the incident report form is a schematic of the facility overlaid by a grid and coordinate markers. The reporting officer details the disturbance and indicates on the schematic exactly where the incident occurred.

The incident report is then mapped by a staff analyst, who records the time and location of the incident and the names and cell locations of the inmates involved. Comparing this map with maps and data from previous incidents, the analyst sees that the brawl site also was the scene of a number of disturbances that occurred only in the late afternoon when this area was less supervised. The analyst then links these maps with such additional inmate data as age, race, religion, and possible gang affiliation. It now appears that the fight may not have been random but instead was the result of an ongoing dispute between rival groups.

Taking the investigation a step further, the analyst overlays a map of inmates who have tested positive for drugs in the past year, then a map of the flow of money in and out of the inmates’ accounts. The picture that now emerges is one of a turf war for control of the drug trade within the prison.

This scenario comes from the prison of the future—a prison that will take full advantage of the warehouse of information it maintains and then use that data to create a comprehensive inmate analysis system (GIS) to link mapping and spatial analysis to the data. But this prison is not that far in the future. Its prototype is in development through a joint project between 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).

Although crime mapping already is used extensively by law enforcement, a major hurdle to using mapping in prisons is the cell-above-cell construction of the living areas. GIS, which operates in two dimensions, cannot be used in prisons because of the multiple levels in many of the buildings. SRTC engineers are working with corrections personnel on staff at NLECTC–Southeast and its regional advisory council have solved this problem by integrating CAD (computer-aided design) technologies, which offer a third dimension. The combination of GIS and CAD technologies allows each cell to be displayed on a computer screen as a separate, identifiable living unit. Individual inmates can thus be shown by referencing them to their assigned beds. This corrections mapping, or CORMAP, instantaneously displays the bed location and available information (data linking) for an inmate when the operator clicks on a bed on the map or enters the inmate’s name or number.

Although corrections mapping is not yet at the stage described in the scenario above, it is capable of tracking and displaying violation patterns, medical information, religious affiliations, cell location, and other inmate data. “You can color-code cells and see interesting relationships,” says Larry Koffman, Ph.D., principal engineer at SRTC. “If you’re getting ready to assign a new inmate, you can quickly display an inmate location map to spot any potential conflicts within the housing unit you’re considering. That’s what GIS lets you do—link graphics with tabular information.”

Koffman says corrections mapping can be useful in situations in which contagious diseases are a problem. An analyst can list an inmate’s previous cellmates (primary contacts), with whom those previous cellmates lived (secondary contacts), and with whom those people lived (tertiary contacts), as far back as records allow. Given a known source, mapping can trace the course of the disease through the prison system and provide information to prevent further contamination.

Mapping programs also can help prison officials deal with the tremendous amount of inmate movement. “We release several thousand inmates each year, either as a result of parole or discharge,” says John Taylor, a former assistant warden now in charge of the Virginia Department of Corrections’ Offender Management Automation System project. “When an inmate leaves, he usually is discharged from a lower security facility. So every time an inmate drops a security level, he moves. This means somebody else has already moved out of that spot. This also means someone else has moved into that inmate’s previous cell. In addition, there might be an inmate conflict in a cell and you have to move somebody. Or an inmate gets sick and has to be moved to a medical facility. We have a lot of inflow and outflow; we need to be able to track inmates’ movement through the system.”

Mapping and analysis programs prove the adage that a picture is worth a thousand words. Proponents foresee a time when corrections mapping can be used to—

- Track and display inmate location and movement via electronic monitoring devices.
- Indicate whether a housing unit is balanced with regard to religion, group affiliation, age, race, and ethnicity.
- Pinpoint the locations of gang members and link them to each inmate’s behavioral and criminal history, as well as the inmate’s rank in the hierarchy of the group. (This would allow for segregation or lockdowns as necessary, which is especially important because committing violent acts is how an inmate moves up in the rank structure of certain groups.)
- Pinpoint areas in a facility that are potentially dangerous, such as hallways or blind corners where a number of assaults have occurred. (Identifying those areas might lead administrators to put additional officers or security devices in the area, increase the lighting, or reroute foot traffic.)
- Incorporate aerial photos of the facility to check for possible security breaches and potential escape routes.
- Provide a basis for proactive investigation and enforcement. (For example, mapping the flow of money in and out of a facility and then linking this information with data about visits, telephone calls, and corresponding addresses could show a potential drug problem.)
- Link inmate data with the names, telephone numbers, and addresses of all the people the inmate had contact with during incarceration, in case of an escape.

There are, however, several roadblocks that need to be overcome before a correctional facility can fully use a mapping and analysis system. Unlike law enforcement, which uses latitude and longitude to pinpoint an event, a correctional institution has no such coordinates. Although some newer facilities offer detailed blueprints that can be assigned coordinates, older ones do not have these blueprints. In addition, although cell blocks and buildings may have names, their interiors do not have addresses like those assigned to homes and buildings. Corrections administrators and program developers will have to find a way to put markers or “addresses” on the walls or floors of a facility. Correcting mapping also will require reports to include specific information about incident location. Information now recorded is often too vague to be usable.

The advantages of implementing a mapping and analysis system, however, will be significant. “It would give us the advantage that otherwise would sit in a warehouse and gather dust,” says Taylor.

“We won’t have to be constantly updating wall maps,” says Ken McKellar, division director of security for the South Carolina Department of Corrections. “We won’t have to sort through and translate raw data. We’ll be able to push a button and get the information we want.”

According to Rob Donlin, who heads up the CORMAP project for NLECTC–Southeast, the idea of a mapping and analysis program for corrections has been met with great enthusiasm. NLECTC–Southeast staff have presented information about CORMAP at conferences and workshops. Donlin says they have been inundated with calls from correctional institutions around the country, all offering their facility as a testbed. “We’re now working on the program’s information links, and then we’ll get the test institutions,” Donlin says. “Once the CORMAP design is complete, we’d like to get it out into the field as quickly as possible.”

For more information about corrections mapping, contact Rob Donlin at NLECTC–Southeast, 800–292–4385, or e-mail donlin@nlectc-se.org.
A 38-year-old man was arrested early this year when law enforce-
ment officers discovered a missing 13-year-old Pennsylvania girl
bound to a bed in his rented house in Virginia. The man, a systems
program analyst, met the young teenager on the Internet and per-
suaded her to meet him in person on New Year’s Day, police say.

A family was surprised to find U.S. Secret Service agents at their
door one morning. Their teenage boy had brought home expensive
computer equipment that he said came from swap meets. It did not.
The boy purchased the equipment over the Internet with an un-
authorized credit card. Evidently, he then used his computer to
e-mail a threatening message to the President.

The role of the law enforce-
ment officer is to protect the com-
munity, particularly its children,
but when the community expands
to include the virtual world of the
Internet, providing that protection
presents a new set of challenges.

Children and teenagers are the
fastest growing group of Internet
users, with an estimated 45 million
expected to be online in 2002. The
number of Internet crimes against
children is growing almost as rapid-
ly. A survey of children ages 10 to
17 found that 1 in 5 had received an
unwanted sexual solicitation in the
past year, and 1 in 33 had received an
aggressive solicitation for offline contact.1 Pornographers entice
children to visit their websites by
disguising them with popular chil-
dren’s brand names like Disney®
or Barbie®.2 Seventy-five percent
of children are willing to provide
personal information about them-
selves and their families in ex-
change for goods and services.3

Computers are a permanent
part of children’s lives. Even if the
home has no computer, a child may
have access to the Internet at
school, the library, or a friend’s
home. To help protect children who
are online, Det. Leanne Shirey, a 23-
year veteran of the Seattle Police
Department, developed a class that
provides the information and tools
needed by parents, teachers, and
others to supervise children’s
online experiences and protect
them from online victimization.

The class was developed after
Shirey tried to find information on-
line that addressed supervision of
children on the Internet. Although
the Internet provides good re-
sources, Shirey says, too many par-
ents either do not know how to
access the information or, when
they do, they find only brief or
generic information that does not
answer their specific questions. So
Shirey and her fellow officers pulled
information they thought
parents should know and organized
it into a 7-hour lecture and hands-
on class they call The Internet
and Your Child.

Shirey says the need to arm
parents with basic skills and knowl-
edge about the Internet is clear.
As she and her fellow officers inves-
tigated cases of children who had
been victims of sexual predators on
the Internet, they found obvious evi-
dence in the homes that something

---

1Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak, Online Victimization: A Report
on the Nation’s Youth (Conducted by the Crimes Against Children Research Center at the
University of New Hampshire, for the National Center for Missing and Exploited Children
2Cyveillance (www.cyveillance.com).
3eMarketer™ (www.emarketer.com).
The Internet and Your Child

The Internet and Your Child class is organized into modules. Each section builds on the next, so it can be used in any setting, from a PTA meeting to a law enforcement group, or for a 5-minute talk or an hour-long briefing. The material is interactive and hands-on.

Offered at no cost, the class begins with the basics. It discusses the issues of managing technology in the home and provides a guide and forms for parents to use in creating their own Internet rules. One obvious rule is to require that the computer be in a public room. Parents should tell their children that they should stand behind the computer in the house with the screen turned toward the center of the room. Class participants are shown to set the toolbar so they can observe what children are doing online and to use the browser history or drop-down menu. “If the drop-down menu bar is empty, you have to ask why,” Shirley says.

Another rule for children is never to provide personal information such as names, addresses, or phone numbers on the Internet. Predators are patient and keep carefully gathered information about their chat room contacts. For example, children who sign off a chat room saying they have to go because their mom is home or because it is time to go to baseball practice are providing clues to the predator. A child may inadvertently give another child’s name and address. If the family vacation will be. Predators save this seemingly innocuous information in an address book as the many sources of personal information on the Internet to identify potential victims.

Class participants also learn to search chat rooms, read an Internet address, deal with issues of property rights and ethics, and identify scams and schemes. They learn how to use monitoring and filtering software programs and how a child could get around the software. Filtering software, Shirley says, is used to restrict access to adult Internet sites, while monitoring software runs behind the computer operating system and is activated when the computer is turned on. It records all keystrokes, including instant messaging and chat room conversations, without slowing or changing computer performance.

As part of the class, the instructor posts a teenager goes online and into a chat room to demonstrate how quickly predators approach their young targets. “They always do,” Shirley says. “In every class.”

The Internet and Your Child class does not focus solely on children as victims. It also looks at the problem of children predators and uses the signs that a child may be involved in online criminal activity.

“Children think computers are like video games,” Shirley says. “They forget judgments and the safety rules they routinely follow in the physical world and think they don’t apply to the cyber world. It is so tempting to think children and their parents understand the ethics of the Internet and the concepts of privacy and ownership—that it’s not all right to steal music from the Internet or hack into a company’s website for fun. Kids will use a password they find where Internet hackers or gaming sites without considering whether they have the right to use it. This is no different from finding a key on the sidewalk and using it to open your neighbor’s front door. When kids who are caught hacking a website excuse their behavior by claiming that they did no damage, I ask them if they would consider it intolerable to break into a neighbor’s house if they just were looking around.”

An issue that comes up in almost every class is whether parents should have password access to their child’s e-mail account. Shirley says they should. “You do things in the physical world to keep an eye on your children. Being aware of who’s contacting your child online is not spying. You have to eliminate secretive behavior.”

Training the Trainer

A problem soon developed with The Internet and Your Child class. The demand for the class was greater than the number of available instructors. So Shirley and her coworkers took the original material and made it part of an intensive, 4-day course that certifies individuals to offer the class to others. Although there is a $150 fee for the train-the-trainer course, the fee is waived when participants present the class in their communities. To participate in the course, all would-be trainers must provide a brief resume and be screened by a computer knowledge and prior training skills and experience, and people skills. The students in each class are a blend of law enforcement officers and investigators, corporate and Internet safety officers, and private individuals.

In October 2000, Wilma Jolly, a program coordinator at the National Law Enforcement and Corrections Technology Center (NLECTC)–West, conducted one of the train-the-trainer courses. Jolly attended 3 days of classroom training and 1 day of computer hardware and software basics, accessing the Internet, passwords, e-mail, newsgroups, chat rooms, Internet addressing, hacking, fraud, sex crimes, ethics, privacy, copyright and licensing issues, searching and filtering and blocking software.

“I had never been in a chat room,” Jolly says. “We went in as if we were a 14-year-old and immediately we were approached by a 27-year-old man and he gave explicit detail as to what sexual acts he wanted to perform.”

Jolly says on the fourth day, participants teamed up and presented The Internet and Your Child class as their “final exam.” Their presentations were videotaped. After a review of the videos, participants were given their certification—or not—as trainers for The Internet and Your Child.

Participants in Jolly’s class included parents, a school safety and security officer, and a PTA representative, a casino representative, and police officers and sheriffs from jurisdictions in Colorado, Kansas, and Texas. Following Jolly’s training, NLECTC–West hosted train-the-trainer courses.

Since its inception, The Internet and Your Child has been offered in 16 States and has been used as a model in several other training courses. The training is now part of the department’s Internet Task Force and is used as a model in several other task forces. Instructors are volunteer law enforcement officers, computer specialists from the community, and graduates who have been certified through the train-the-trainer course. Classroom space equipped with computers often is donated by corporations and schools. Participants receive a manual filled with references and additional information from the Federal Government and other sources. The training is designed to aid law enforcement agencies in identifying the sources of personal information on the Internet and to aid them in fighting computer and electronic crime.

Following the success of this class, Waldron says, the Federal Bureau of Investigation (FBI) asked NLECTC–West to host a 2-week class for Internet investigators. He contracted classroom space and high-speed Internet access that the FBI did not have, and his staff were able to build relationships with investigators from other agencies in the region.

In addition, Waldron says NLECTC–West is an active member in the Southern California High Technology Task Force Steering Committee, serving as its secretariat. The steering committee is composed of industry representatives who provide insight and guidance to the task force on the state of electronic crime in the region. The center also has been coordinating the Governor of California’s statewide monitoring group and was invited to give a presentation on the NLECTC system and its role in supporting law enforcement agencies working on electronic crime cases. Following Waldron’s presentation, the Los Angeles Electronic Crime Task Force, which is being organized under the aegis of the U.S. Secret Service under the USA Patriot Act, invited the center to present a similar training program in Los Angeles.

Waldron says NLECTC–West currently is involved with five electronic crime task forces. This includes the Los Angeles Electronic Crime Task Force, which was recently established. This forensic casework has naturally evolved into the center’s work with electronic crime issues and the task forces that have been created to deal with this burgeoning problem. Because the availability of training is a continuing problem for task force investigators, Waldron says his center has taken the initiative to host various training opportunities.

NLECTC–West was created under the White Collar Crime Initiative to offer a weeklong course on the basics of computer data recovery to investigators from seven western States at the Aerospace Corporation, NLECTC–West’s technology partner, in Los Angeles, California. The class was so successful it was repeated at two other NLECTC system facilities.

Following the success of this class, Waldron says, the Federal Bureau of Investigation (FBI) asked NLECTC–West to host a 2-week class for Internet investigators. He contracted classroom space and high-speed Internet access that the FBI did not have, and his staff were able to build relationships with investigators from other agencies in the region.

In addition, Waldron says NLECTC–West is an active member in the Southern California High Technology Task Force Steering Committee, serving as its secretariat. The steering committee is composed of industry representatives who provide insight and guidance to the task force on the state of electronic crime in the region. The center also has been coordinating the Governor of California’s statewide monitoring group and was invited to give a presentation on the NLECTC system and its role in supporting law enforcement agencies working on electronic crime cases. Following Waldron’s presentation, the Los Angeles Electronic Crime Task Force, which is being organized under the aegis of the U.S. Secret Service under the USA Patriot Act, invited the center to present a similar training program in Los Angeles.

Waldron says NLECTC–West currently is involved with five electronic crime task forces. This includes the Los Angeles Electronic Crime Task Force, which was recently established. This forensic casework has naturally evolved into the center’s work with electronic crime issues and the task forces that have been created to deal with this burgeoning problem. Because the availability of training is a continuing problem for task force investigators, Waldron says his center has taken the initiative to host various training opportunities.
Technology can significantly enhance the effectiveness and efficiency of law enforcement, corrections, and forensic sciences. Just as important, it can help ensure public safety. But the incorporation of new technology can be complicated and require significant research, while inappropriate or underutilized technology can be costly—not only in money but also in time and public perception.

The National Law Enforcement and Corrections Technology Center (NLECTC) system, a program of the National Institute of Justice, can help agencies large and small when it comes to implementing current and emerging technologies. NLECTC serves as an “honest broker” resource for technology information and support at no cost.

Because most of this 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. These centers and offices are co-located or supported by federally funded technology partners so they can leverage unique science and engineering expertise.

Contact NLECTC for:

Technology Demonstration
NLECTC introduces and demonstrates new and emerging technologies through such special events, conferences, and 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.

Training Assistance/Capacity Building
NLECTC provides hands-on instruction in the latest technology solutions, primarily in the areas of crime and intelligence analysis, geographic information systems, explosives detection and neutralization, inmate disturbances and riots, and computer crime investigation.

Technology Commercialization
Bringing research and private industry together to put affordable, market-driven technologies into the hands of law enforcement and corrections personnel is another focus of NLECTC. Law enforcement and corrections professionals, product and commercialization managers, engineers, and technical and market research specialists identify new technologies and product concepts, then work with innovators and industry to develop, manufacture, and distribute these new, innovative products and technologies.

Technology Needs Assessment/Prioritization
A national body of criminal justice professionals—the Law Enforcement and Corrections Technology Advisory Council (LECTAC)—influences the work of the

Technology Identification
As an agency’s first stop in its search for new and developing technologies, NLECTC provides information relating to availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability. This information helps an agency determine the most appropriate and cost-effective technology to solve an operational problem.

Technology Assistance
Because most law enforcement and corrections agencies do not have access to technical experts and sophisticated equipment, NLECTC staff serve as proxy scientists and engineers. Areas of assistance include 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/Property Acquisition
For most small departments, the acquisition of equipment to run day-to-day operations or outfit officers is a constant concern. NLECTC helps departments small and large 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.

Standards and Testing/Technology Evaluation
NLECTC oversees a standards-based testing program in which equipment such as ballistic and stab-resistant body armor, double-locking metallic handcuffs, and semi-automatic pistols is tested on a pass/fail basis. NLECTC also conducts comparative evaluations—testing equipment under field conditions—on patrol vehicles; patrolled vehicle tires and replacement brake pads; and cut-, puncture-, and pathogen-resistant gloves. These evaluations allow agencies to select equipment that best suits their needs. On request, NLECTC evaluates new products to verify manufacturers’ claims.

Technology Information Dissemination
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 newsletter. Most publications are available in electronic form through the Justice Technology Information Network (JUSTINET) at www.justinet.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.

NLECTC system by identifying research and development priorities. In addition, each regional facility has an advisory council of law enforcement, corrections, and forensics professionals. Together, LECTAC and the regional advisory councils help keep the NLECTC system attentive to real-world technology priorities and the needs of law enforcement and corrections. Created in 1994 as a program of the National Institute of Justice’s (NIJ’s) Office of Science and Technology, the NLECTC system’s goal, like that of NIJ, is to offer support, research findings, and technological expertise to help State and local law enforcement and corrections personnel do their jobs more safely and efficiently.
In addition to funding the National Law Enforcement and Corrections Technology Center, the National Institute of Justice (NIJ) supports the National Criminal Justice Reference Service (NCJRS), an international clearinghouse on crime and justice information. NCJRS staff respond to reference questions, provide referrals to other resources, distribute NIJ and other Office of Justice Programs (OJP) documents, and maintain a mailing list of more than 45,000 registered users.

In addition, NCJRS sponsors a calendar of events at www.eventcalendar.ncjrs.org, which lists conferences and meetings of interest to the criminal justice community. If you are interested in signing up for the NCJRS mailing list, you may request a registration form using any of the following methods:

- **Fax-on-Demand**: Dial 800–851–3420, select option 1, then option 1 again. The registration form is #1 on the document index. The form will be faxed to you immediately.
- **Fax**: Fax your request for a registration form to 410–792–4358. You will receive a form promptly in the mail.
- **Online**: Go to www.ncjrs.org/puborder and request registration form BC640. It will be sent to you in the mail. Or register online at www.ncjrs.org/register.
- **Write**: Send a written request to NCJRS, P.O. Box 6000, Rockville, MD 20849–6000.
- **Call**: Call an NCJRS information specialist at 800–851–3420 and request a registration form.

As a registered user, you will receive the bimonthly NCJRS Catalog, the NCJRS Users Guide, and news and announcements of new publications and resources based on your criminal justice interests.

For more information about NIJ and NCJRS, visit their websites: www.ojp.usdoj.gov/nij and www ncjrs.org.

The following publications are available from the National Law Enforcement and Corrections Technology Center–National:

**National Law Enforcement and Corrections Technology Center Publications Catalog 2002.** This document provides a listing of NLECTC and other government publications of interest to law enforcement, corrections, and forensic sciences practitioners. Categories include communications, forensics, less-than-lethal weapons, protective equipment, and weapons and ammunition.

**2002 Model Year Patrol Vehicle Testing.** This report contains the complete results of comprehensive tests of 2002 model year police patrol vehicles conducted by the Michigan State Police.

**Equipment Performance Report: 2001 Patrol Vehicle Tires.** This report presents the complete results of NIJ’s 2001 comprehensive evaluation of patrol vehicle tires.

**TechBeat, Spring 2002.** This TechBeat features drug testing technologies; the Web Enabled Timeline Analysis System and how it aided a murder investigation; funding resources available from the Office of Justice Programs and the Office of Community Oriented Policing Services; and JUSTNET, the website of NLECTC.

**TechBeat, Winter 2002.** Articles discuss counterterrorism initiatives; the two newest facilities to join the NLECTC system and their specialties; Fuginet, a database that can identify and track parole violators; and tools to help investigators keep pace with the growing number of crimes involving electronic evidence.
Prisoners’ Mugshots Go Online

Detroit Free Press Online

Michigan Department of Corrections (MDOC) spokesman Matt Davis says the department’s website will soon include roughly 37,000 new images of inmates and parolees, with more mugshots to be added later. Additionally, expansion of the Offender Tracking Information System database will cover information relating to inmates’ crimes, sentences, and release dates. Davis says expansion of the website will give the public greater access to information. Besides public use, the department also expects other agencies, such as law enforcement and social services, to access the database more often. However, Davis notes the service will only make information available that is currently on public record. Users can access mugshots by clicking on the offender search button at the MDOC site, www.michigan.gov/corrections.

Multi-Agency Nevada Cybercrime Lab Opens in Las Vegas

Associated Press

A new Cyber Crime Task Force laboratory was launched late last year as part of Nevada’s participation in the FBI’s InfraGard program that aims to investigate, protect against, and provide information about computer crimes. Gov. Kenny Guinn noted that everyday Internet participation in the FBI’s InfraGard program that launched late last year as part of Nevada’s participation in the program provided the impetus for the new laboratory.

A new Cyber Crime Task Force laboratory was launched late last year as part of Nevada’s participation in the FBI’s InfraGard program that aims to investigate, protect against, and provide information about computer crimes. Gov. Kenny Guinn noted that everyday Internet participation in the FBI’s InfraGard program that launched late last year as part of Nevada’s participation in the program provided the impetus for the new laboratory.

The Shadow War

Popular Science

New scanning systems are the most promising long-term solutions for analyzing air passengers and their bags. One of the most high-profile systems is the face-recognition system, which is currently being used in several places around the country. A specialized form of the system, HumanID, is being tested by the Defense Advanced Research Projects Agency (DARPA). The system uses face recognition in combination with other surveillance techniques. HumanID is also able to alert authorities when an individual appears at a site on numerous occasions, such as a terrorist casing an airport. In addition, DARPA is using Dragon Eye, a miniature plane equipped with video cameras and a GPS locator able to radio images and their location back to the operator.

FBI Sets ‘Aggressive Hiring’ Goal at 900; Languages, Cyber-Skills Are Priorities

Washington Technology

The FBI wants to hire up to 900 new law enforcement agents by the end of September. The agency already is reorganizing its Washington, D.C., headquarters, and FBI Director Robert S. Mueller noted the overhaul will include implementation of new technology and shifting focus of existing assets. The agency will focus on hiring agents specializing in engineering, physics, chemistry, biology, or other important fields. Candidates also will be able to fluently speak any number of languages, including Pashtu, Arabic, Chinese, Korean, Russian, and Vietnamese. The bureau also is launching four new offices to improve communications with State and local law enforcement agencies. In addition, the offices will aid technology projects, upgrade FBI records, and improve intelligence capabilities.

Judge OKs FBI Keyboard Sniffing

Wired News

U.S. District Judge Nicholas Politan ruled that the FBI could legally install a keystroke logger in the PC of alleged mobster NicocurrentPage 1 of 21 in the Uniform Crime Report System. The logger will be used to collect data from the computer’s keyboard. The FBI has sought to install the logger in order to gather evidence against an alleged mobster.

New Web Site Supports Local Law Enforcement

Washington Technology

The U.S. Department of Justice has initiated a website intended to help State and local law enforcement agencies and the public in the campaign against crime. Formed by the Bureau of Justice Statistics, the website offers easy-to-interpret sets of criminal information for access by State and local law enforcement, government officials, and the public at large. Users can obtain information on the site from the FBI’s Uniform Crime Reports and Supplemental Homicide Reports, and from the Law Enforcement Management and Administrative Statistics. Users can make data tables on criminal violations from the Uniform Crime
The technology uses robots equipped with a video camera, a microphone, a wireless transmitter for sending signals to an Internet connection, artificial intelligence software, and sensors. Telepresence robots allow users to go online from their remote location and see what the robots see and hears. Users also can use a mouse to control the movements of the telepresence robot. A firm called iRobot plans to sell telepresence robots for both business and home use. There are some concerns that people will have a hard time embracing telepresence robots because they are likely to see them more as camera-wielding intruders. However, telepresence robots may offer benefits that are so great, such as safe alternatives for seniors who do not want to live in nursing homes, that people may come to accept them. So far, reconnaissance in dangerous environments, such as the World Trade Center site, appears to be the best demonstration of the value of telepresence robots, and the Defense Advanced Research Projects Agency has decided to fund an iRobot telepresence robot that specializes in reconnaissance and surveillance.

Why Worm Writers Stay Free

Wired News

Although many virus writers may openly boast of their activities or leave calling cards, law enforcement officials are having a tough time bringing them in. Tracking down worm authors is often easier said than done. Last year, computer security experts, shipping, and mail services, as well as the U.S. Army, Navy, and Federal Aviation Administration, and various water utilities, oil companies, and even nuclear facilities have requested demonstrations of the technology. At least, the sensors can be programmed to emit a high-volume noise if any motion is detected; more complicated applications include using a computer to analyze the noise frequency to determine how big the intruder is and where the breach took place, as well as training surveillance cameras or even releasing tear gas at the location.

Long-Distance Robots

Scientific American

Radar could make up for some of the shortcomings of videoconferencing, such as the difficulty of understanding what participants are saying and the lack of equipment mobility.

The province of computer security experts, many of whom are too busy trying to stay ahead in the midst of the recession to help investigations. However, the culprits usually leave obvious clues to their identities, and it is merely a matter of someone noticing and alerting the proper authorities. For example, the Israelis autho...
The MOLE Programmable Detection System, manufactured by Global Technical Ltd., of Kent, England, is advertised as a device capable of detecting a number of substances (e.g., drugs, explosives) simultaneously or one at a time.

To “program” the product for detecting one or more substances, the operator inserts the appropriate programming cards into a cardholder clipped to the operator’s belt. The cardholder is attached to a search handle by a short cable with standard phone jacks on each end. The search handle is a small black plastic handle with a radio-type antenna mounted in a free-turning pivot. When the antenna is fully extended, it can be balanced to protrude in front of the operator but is free to swing to either side with the slightest tilt of the operator’s hand.

Sandia National Laboratories evaluated the explosive detection capability of the MOLE in a double-blind field test in January 2002 at the National Law Enforcement and Corrections Technology Center–Rocky Mountain in Denver, Colorado. Test results, in addition to subsequent quality assurance checks, indicated that, for this purpose, the device “performs no better than a random selection process,” or random guessing.

For the double-blind tests, approximately 20 grams of C4 explosives were placed in a plastic bag with a twist top and enclosed in a plastic 35-mm film canister. To ensure that no contamination affected test results, surfaces used during the test were tested for the presence of explosives contamination using an ion mobility spectrometer. The results of the ion mobility spectrometer test indicated there was no contamination that might interfere with the test.

To view or download a copy of the full report, Double-Blind Field Evaluation of the MOLE Programmable Detection System, log on to JUSTNET at www.justnet.org. For specific questions relating to testing methodology, contact Dale Murray, Entry Control and Contra-band Detection Department, Sandia National Laboratories, at dvmurra@sandia.gov or 505–845–8952.

Editor’s Note: In October 1995, Sandia National Laboratories examined a product that appeared physically nearly identical to the MOLE. This product was the Quadro Tracker, which was manufactured by the Quadro Corporation of Harleyville, South Carolina. The visible physical differences between the two products appeared to be the product labels and the handle-programming chip. On the Quadro Tracker, the programming chip was interchangeable and could be inserted into the handle; on the MOLE, the programming chip is permanently fixed into the handle.

Additional information on the Quadro Tracker can be located by searching the Internet using the keywords Quadro and Tracker.