Wayne County covers 484 square miles of rolling hills in south central Kentucky. Fewer than a dozen deputies of the Wayne County Sheriff's Office provide law enforcement services to more than 20,000 of their fellow citizens. Like other agencies in rural and remote areas, it lagged behind its more affluent metropolitan counterparts in access to and use of new technologies until the sheriff's office revamped its operations—with assistance from the Rural Law Enforcement Technology Center (RULETC).

Just 3 years ago, the Wayne County Sheriff's Office had only one computer, which was 20 years old and used solely for tax records, says Doug Dailey, a program manager at RULETC. Using the 1033 Program, which makes excess U.S. Department of Defense property and equipment available to law enforcement agencies, the Center helped the sheriff's office acquire 14 laptop and personal computers, boosting the agency's efficiency and effectiveness.

With the computers, deputies can now use a number of computerized report forms provided by the Kentucky State Police, as well as accident reporting and investigation software. In addition, the sheriff's office can now participate electronically in the Kentucky Incident Based Reporting System (KYIBERS), a statewide network that collects, edits, and stores uniform crime reports from all Kentucky law enforcement agencies and reports these data to the Federal Bureau of Investigation. The laptops enable personnel to attach digital photos to the reports and to relegate to the past the errors, illegibility, and submission lag time of handwritten reports. The computers also allow deputies to perform crime and incident mapping using global positioning systems (GPS) and to access information on civil and criminal complaints available on COURTNET, a group of secure websites hosted by the Kentucky Court of Justice and the Administrative Office of the Courts.

In addition to the computers, RULETC helped the sheriff's office acquire two 4x4 trucks and a number of night-vision goggles, which have enhanced, among other things, the agency's marijuana eradication performance. According to Dailey, the agency can identify and locate a suspected grower using information from COURTNET, monitor nighttime activity with the goggles, pinpoint the grow area with GPS, notify other agencies via e-mail, and haul away seized evidence in the offroad vehicles.

The 4-wheel-drive trucks, Dailey says, also come in handy for other police operations, such as transporting inmates on work detail and patrolling in bad weather. When a heavy snowstorm prevented cruisers from navigating the roads this past winter, the 4x4 trucks were able to reach areas that were inaccessible to other vehicles.

For years law enforcement and corrections agencies had only three options for dealing with combative individuals: talk them into submission, strike them with a baton, or shoot them with a firearm. Today, agencies have more options at their disposal—less-lethal technologies such as chemical irritants and inflammatories, impact munitions, and, most recently, electro-muscular disruption technology (EMDT).

EMDT devices deliver a high-voltage (up to 50,000-volt), low-powered electrical charge to induce involuntary muscle contractions that cause temporary and reversible incapacitation. According to Dailey, the agency can identify and locate a suspected grower using information from COURTNET, monitor nighttime activity with the goggles, pinpoint the grow area with GPS, notify other agencies via e-mail, and haul away seized evidence in the offroad vehicles.

The 4-wheel-drive trucks, Dailey says, also come in handy for other police operations, such as transporting inmates on work detail and patrolling in bad weather. When a heavy snowstorm prevented cruisers from navigating the roads this past winter, the 4x4 trucks were able to reach areas that were inaccessible to other vehicles.

Over the past decade, more than 5,000 departments have turned to EMDT to augment their less-lethal force options. Although manufacturers assert that the use of EMDT has no residual medical effects, increased deployment of the devices...
winter, the trucks were not only used to perform normal patrol functions—one also was used to transport an injured elderly woman to the hospital.

In addition to providing 1033 Program assistance, RULETC maintains a mobile interactive, judgmental shooting simulator with a laser-guided shootback feature. Wayne County deputies have used the simulator to hone their use-of-force judgment and practice their shooting skills.

The simulator places law enforcement personnel in simulated real-time situations in which they have to react to a scenario as it unfolds, requiring split-second decisions as to whether or not to use deadly force.

“The system logs where and when an officer fires in relation to a perpetrator, providing feedback on accuracy and reaction time, and the shootback feature helps to reinforce the need to use available cover,” Dailey says. “The best part of the simulator is that the computer operator can vary a scenario to test an individual’s judgment in deciding whether or not to use deadly force. As important as accuracy is, correct judgment in deciding when to shoot is more important. The simulator helps develop this skill.”

Wayne County Sheriff’s Deputy Terry Davis credits its use of the simulator with saving his life. While helping the sheriff’s department of adjacent Clinton County in a stolen truck incident, Davis set up a roadblock by parking his cruiser across the highway to stop the approaching vehicle. “I thought the driver was giving up, and I got out of my car. Then I thought I saw him raise a revolver, and I realized that I had forgotten my concealment.”

On instinct, he fired one shot and retreated behind his cruiser, planning to set up for a better shot. In the meantime, the suspect turned his vehicle around and sped off. Davis decided to resume the chase rather than fire again. The entire episode lasted no more than 10 seconds. “I responded to the threat like I had been trained to do and felt good about my ability to react to a deadly threat,” Davis says.

Davis has run through most of the simulator’s 500 scenarios at least once. Many of them take place in rural settings similar to Wayne County. Davis appreciates that he can use a weapon in the simulator that is like the one he uses on the job and that the self-study program allows him to proceed at his own pace. Davis even used his surplus laptop and accident investigation and reconstruction software to recreate the incident for his sheriff and fellow deputies.

Wayne County Sheriff James Hill stresses to his staff the importance of training and using technology. Dailey adds, “RULETC exists to help agencies like the Wayne County Sheriff’s Office build their capacity, add to their resources, and meet their information and technology needs.”

RULETC, located in Hazard, Kentucky, is part of the National Institute of Justice’s National Law Enforcement and Corrections Technology Center system. In cooperation with its technology partner, Eastern Kentucky University, the Center provides technology solutions to a historically underserved population—the Nation’s 13,000 rural, small town, and small county criminal justice agencies. For more information, call 866-787-2553 or e-mail ruletc@aol.com.

In addition to the 1033 Program, State and local law enforcement agencies can obtain excess Federal property at little or no cost through the 1033 Donation Program and the 1122 Program. For more information about any of these programs, access the Federal Property and Equipment Manual at www.justnet.org/virlib/InfoDetail.asp?intInfoID=170 or contact one of the facilities of the National Law Enforcement and Corrections Technology Center system listed on page 4.

Weeding Out Weed... and Other Drugs

According to the website of the Wayne County, Kentucky, Sheriff’s Office, the area is “well known for the copious amounts of marijuana grown in the county.” Several times during the 1990s, the county was cited as the second largest growing area for marijuana in Kentucky. The sheriff’s office has led the fight against the illegal drug in the county, leading the State in the number of plants cut by a local agency.

Marijuana has become the number one cash crop in Kentucky, Tennessee, and West Virginia, which comprise the Appalachia High-Intensity Drug Trafficking Area (HIDTA), according to the website of the Office of National Drug Control Policy. These three States, with less than 4 percent of the total U.S. population, produced 34.5 percent of the domestic marijuana supply in 2003 (measured in total eradicated plants). Usage rates in the Appalachia HIDTA, however, are below the national average. This indicates that the majority of marijuana cultivated in the region is headed for markets in other areas and that the Appalachia HIDTA represents a major drug threat. In addition, much of this marijuana is grown on public land. Growers intrude on several national forests, as well as lands owned by the Tennessee Valley Authority. Public use of these areas has diminished because of the threat of violence from marijuana growers, but marijuana is not the only problem.

• The Appalachia HIDTA is experiencing a dramatic escalation in the methamphetamine threat. The number of methamphetamine labs dismantled in the region increased from 45 in 1999 to 474 in 2003.
• Cocaine in both powder and crack forms remains a significant drug of abuse in metro-politan and rural areas.
• Prescription drug seizures by Appalachia HIDTA personnel expanded dramatically from 4,706 dosage units in 1999 to 105,757, dosage units in 2003. The trafficking and illicit use of prescription drugs, especially the pain reliever OxyContin®, may well be the most significant drug problem aside from marijuana within the HIDTA.

For more information about the Appalachia HIDTA, as well as the other programs of the Office of National Drug Control Policy, visit www.whitehousetaggedrugs.gov.
has raised concerns about safety, liability, potential misuse, and associated risks.

**Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment** is a new executive brief from the International Association of Chiefs of Police (IACP) that assists agencies in implementing EMDT technology. According to Al Arena, project manager at the IACP’s Research Center Directorate, this executive brief helps law enforcement not only make informed decisions as to whether or not to deploy EMDT devices but also how to deploy them. Arena says the brief alerts agencies to issues involved in using the technology, including the possibility of in-custody deaths, an issue that received a great deal of media attention following a November 2004 report by Amnesty International.

Work on the IACP executive brief, which was funded by the National Institute of Justice (NIJ), began well before the release of the Amnesty International report. However, the release of that report caused IACP to accelerate the pace of its work. The Amnesty International report caused agencies to reconsider the use of EMDTs, driving home the urgent need for guidance on policies, procedures, and protocols.

“Agencies that had deployed EMDT, even if they had not had a fatality, were asked why they didn’t take the technology off the street until more evidence came in,” Arena says. “Agencies that were contemplating a purchase began having second thoughts.” He adds that IACP did not want agencies that had decided to invest in the technology to cancel or postpone their purchases because no guidelines were available. As a result, IACP sped up its research and production efforts to get this executive brief to the field.

IACP worked closely with NIJ and partnered with the Montgomery County (Maryland) Police Department, which already had deployed EMDT and had policies and procedures in place. (Montgomery County is also located near IACP headquarters in Alexandria, Virginia, enabling Arena to learn the technology firsthand by taking a 6-hour EMDT training class and working closely with Montgomery County Police Department Capt. Alan Goldberg, a master EMDT trainer.) Arena also gathered anecdotal information from other law enforcement agencies around the country and classified that information according to key issues.

“We’re not skirting away from the issue that people [who have been subjected to EMDT] have died in custody. Agencies need to be aware that a death could be due to a medical condition [or] drug use, and it might be an indirect rather than a direct result,” Arena says.

“In the end, agencies need to know how to manage the technology. Officers who make the decision to deploy it need to know all the ins and outs. The public needs to be involved in any decision to purchase the technology,” he adds. “We’re not issuing any warnings; we just want people to be aware of all the facts and all the issues.”

**Electro-Muscular Disruption Technology: A Nine-Step Strategy for Effective Deployment** presents a step-by-step guide for law enforcement and corrections agencies that are considering the purchase and use of Electro-Muscular Disruption Technology (EMDT). This executive brief from the International Association of Chiefs of Police does not focus on the technology itself; instead, it emphasizes the management of the technology. Its aim is to help law enforcement leaders develop policies, procedures, and training curricula for EMDT use.

The nine steps are as follows:

- **Step 1: Build the leadership team.**
- **Step 2: Place EMDT on the use-of-force continuum.**
- **Step 3: Assess the costs and benefits of using EMDT.** This involves:
  - Determining whether its use will help reduce serious injuries or deaths to suspects, law enforcement officers, and third parties.
  - Considering whether other effective less-lethal force options are available, whether EMDT use will reduce use of firearms by law enforcement, and whether officers will risk serious injury or death if they try to resolve violent confrontations without less-lethal weapons.
- **Step 4: Identify roles and responsibilities for EMDT deployment.**
- **Step 5: Engage in community outreach.** Although no evidence links serious injury or death directly to the technology, EMDT deployment can be the subject of substantial community and media concern. Deployment plans should acknowledge that community acceptance is essential.
- **Step 6: Develop EMDT policies and procedures.** The policies and procedures should cover training, use, reporting requirements, medical evaluations, legal constraints, and other operational considerations. Policies should also define when use is not appropriate.
- **Step 7: Create a comprehensive training program.** The program would reinforce policies and procedures for EMDT deployment. (For example, many departments require officers who carry an EMDT weapon to experience the electric shock firsthand.)
- **Step 8: Use a phased deployment approach.** Many departments issue EMDT weapons first to special operations teams, such as SWAT or crisis intervention teams, or to supervisors or other select officers.
- **Step 9: Assess EMDT use and determine next steps.** Followup assessments can determine whether the technology is performing as expected and officers are complying with department policies and procedures.

The brief, which includes an appendix of references and resources, can be found at [www.theiacp.org/research/RCDCuttingEdgeTech.htm](http://www.theiacp.org/research/RCDCuttingEdgeTech.htm).
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 serve as an “honest broker” resource for technology information, assistance, and expertise by providing information and technology assistance to the Nation’s more than 18,000 police departments; 50 State correctional systems; thousands of prisons, jails, and parole and probation departments; and other public safety organizations.

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

Contact NLECTC for:

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

Capacity Building
We provide hands-on demonstrations of the latest technologies to address such operational issues as crime and intelligence analysis, geographic information systems, explosives detection and disablement, and technology availability, performance, durability, reliability, safety, ease of use, customization capabilities, and interoperability.

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 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—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 collocated with or supported by federally funded technology partners so they can leverage unique science and engineering expertise.

The NLECTC system was established in 1994 by NIJ’s Office of Science and Technology to serve as an “honest broker” resource for technology information, assistance, and expertise by providing information and technology assistance to the Nation’s more than 18,000 police departments; 50 State correctional systems; thousands of prisons, jails, and parole and probation departments; and other public safety organizations.
A bus driver transporting high school students thought he smelled marijuana. He stopped the bus, secured it, and called school administrators, who alerted the South Texas Specialized Crimes and Narcotics Task Force. Although no marijuana was found, using Hound™ “drug sniffer” technology, officers immediately determined that two pills found on the bus were an illicit substance, allowing the school to resolve the problem immediately instead of waiting weeks for a laboratory analysis.

Since November 2003, the South Texas Task Force has been field testing the Hound system for Sandia National Laboratories. In addition to the school bus incident, the Hound system has saved time, lives, and money on numerous occasions, according to Task Force Commander Jaime Garza.

“Ever since 9/11 we have become more aware of what is being transported along the highway,” says Garza, whose task force operates out of Kingsville, approximately 40 miles south of Corpus Christi. In 2003, the task force approached the Border Research and Technology Center (BRTC), part of the National Institute of Justice’s National Law Enforcement and Corrections Technology Center system, in search of advanced drug detection technology.

According to Director Chris Aldridge, BRTC responded by facilitating the transfer to the task force of the Hound system, a front-end sample collector and preconcentration technology that Sandia developed for use with commercial off-the-shelf drug and explosives detectors. Sandia loaned the equipment to the South Texas task force in exchange for feedback on the system’s operation; Sandia also trained the task force and was available for troubleshooting any problems.

The task force has had plenty of opportunities to test the Hound technology. “In southern Texas we have heat, humidity, and everything else working against us. It’s a good place to test technology, because this is a tough climate,” Garza says. He explains that the task force tries to circumvent heavy traffic in cocaine, heroin, and other hard drugs; it also combats increasing amounts of methamphetamine and their precursors. The South Texas task force operates in a busy area along Highway 77, where the Hound system has played a key role in handling a variety of incidents, such as—

• Identifying liquid and crystal methamphetamine after a routine traffic stop by local law enforcement in summer 2004. The technology not only enabled officers to make a multimillion-dollar seizure, it may have also saved lives because quick identification of the presence of meth enabled officers to immediately treat the incident as a HazMat situation.

• Clearing a tanker truck that had arrived at a nearby military base without the proper inspection seals on its cargo. The technology did not identify the presence of any chemical or explosive substances on the truck, allowing delivery to proceed.

• Locating traces of gunpowder on a decomposing corpse, helping the Texas Rangers with an investigation.

The sample collection and preconcentration technology is a miniaturized version of technology originally developed for the U.S. Transportation Security Administration (formerly the Federal Aviation Administration).

It collects samples by drawing in vapor from the airspace very close to the suspicious object or area; an operator may also swipe a suspicious area to collect a sample. The commercial detector is capable of detecting narcotics in nanogram concentrations (including the residue left in fingerprints). Sandia describes the Hound system as portable, inexpensive, fast, and easy to operate, with a low false alarm rate.

Garza makes it clear that the Hound system is used only with probable cause, and that it is just one tool of many used by his officers. Those other tools include drug-sniffing dogs and a combination of “instinct, experience, and knowledge.”

For more information about the Hound system or other technology initiatives of the Border Research and Technology Center and its technology partner, Sandia National Laboratories, call 888-656-2782 or e-mail info@brtc.nlectc.org.

Q: The commercial detector used in the Hound™ system is capable of detecting narcotics in nanogram concentrations (including residue left in fingerprints). So just how big, or rather, how small is a nanogram?

A: The answer: A nanogram weighs a billion times less than 1 gram. This is equivalent to almost a trillion times less than a pound.
Criminal Intelligence allows law enforcement to collect, analyze, and disseminate information to better understand and combat crime. This information can include anything that is directly or indirectly related to crime, including data on crime, criminals, and criminal activities. The use of criminal intelligence training programs available in the United States, organized by four training classifications:

1. Federal Law Enforcement Training
   - Intelligence Analyst/Officer/Collector
   - Task Force Training
   - Analytical Investigative Techniques
   - Criminal Intelligence Fundamentals
   - Intelligence Analysis Fundamentals for Law Enforcement
   - Intelligence Analysis Fundamentals
   - Intelligence Analysis Fundamentals

2. Regional Countergang and Drug Enforcement Programs
   - Intelligence Analysis
   - Criminal Intelligence Training Coordination Strategy Work Group
   - Federal Bureau of Investigation
   - Intelligence Analysis
   - Criminal Intelligence Training Coordination Strategy Work Group

3. Federal Government Training
   - Intelligence Analyst/Officer/Collector
   - Task Force Training
   - Analytical Investigative Techniques
   - Criminal Intelligence Fundamentals
   - Intelligence Analysis Fundamentals for Law Enforcement
   - Intelligence Analysis Fundamentals
   - Intelligence Analysis Fundamentals

4. State and Local Government Training
   - Intelligence Analyst/Officer/Collector
   - Task Force Training
   - Analytical Investigative Techniques
   - Criminal Intelligence Fundamentals
   - Intelligence Analysis Fundamentals for Law Enforcement
   - Intelligence Analysis Fundamentals
   - Intelligence Analysis Fundamentals

The following programs are open to law enforcement personnel nationwide:

Federal Law Enforcement Training Center

- Intelligence Analyst/Officer/Collector
- Task Force Training
- Analytical Investigative Techniques
- Criminal Intelligence Fundamentals
- Intelligence Analysis Fundamentals for Law Enforcement
- Intelligence Analysis Fundamentals
- Intelligence Analysis Fundamentals

Regional Countergang and Drug Enforcement Programs

- Intelligence Analysis
- Criminal Intelligence Training Coordination Strategy Work Group
- Federal Bureau of Investigation
- Intelligence Analysis
- Criminal Intelligence Training Coordination Strategy Work Group

Federal Government Training

- Intelligence Analyst/Officer/Collector
- Task Force Training
- Analytical Investigative Techniques
- Criminal Intelligence Fundamentals
- Intelligence Analysis Fundamentals for Law Enforcement
- Intelligence Analysis Fundamentals
- Intelligence Analysis Fundamentals

State and Local Government Training

- Intelligence Analyst/Officer/Collector
- Task Force Training
- Analytical Investigative Techniques
- Criminal Intelligence Fundamentals
- Intelligence Analysis Fundamentals for Law Enforcement
- Intelligence Analysis Fundamentals
- Intelligence Analysis Fundamentals

The following programs are open to law enforcement personnel nationwide:

Florida Department of Law Enforcement
- Intelligence Analyst Curriculum
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis

Regional Information Sharing Systems

- Regional Information Systems

National Drug Intelligence Center

- Introduction to Basic Drug Intelligence Analysis
- Intelligence Analysis Fundamentals for Law Enforcement
- Intelligence Analysis Fundamentals
- Intelligence Analysis Fundamentals

California Department of Justice
- Intelligence, Basic Elements
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis

U.S. Drug Enforcement Administration
- Intelligence Analyst Curriculum
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis

The following programs are open to law enforcement personnel nationwide:

Institute for Interagency Training
- State and Local Anti-Terrorism Training Program (SLATT)
- SLATT Program
- SLATT Program
- SLATT Program

U.S. Drug Enforcement Administration
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis

The following program is open to law enforcement personnel from specific agencies or geographic areas:

High Intensity Drug Trafficking Areas
- Local Law Enforcement Personnel
- High Intensity Drug Trafficking Areas
- Local Law Enforcement Personnel
- High Intensity Drug Trafficking Areas

The following programs are open to law enforcement personnel nationwide:

Institute for Interagency Training
- State and Local Anti-Terrorism Training Program (SLATT)
- SLATT Program
- SLATT Program
- SLATT Program

U.S. Drug Enforcement Administration
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis
- Criminal Intelligence Analysis

The following program is open to law enforcement personnel nationwide:

Institute for Interagency Training
- State and Local Anti-Terrorism Training Program (SLATT)
- SLATT Program
- SLATT Program
- SLATT Program
Institute for Intergovernmental Research

- Criminal Intelligence for the Chief Executive. This 4-hour course, which is in the pilot program phase, will provide a briefing to executive-level personnel regarding the National Criminal Intelligence Sharing Plan, intelligence-led policing, basic intelligence issues, legal issues, and available resources. http://www.iir.com/

The following program may be limited to law enforcement personnel from specific agencies or geographic areas.

California Department of Justice

- Criminal Intelligence for Executives. This 16-hour course provides law enforcement administrators in California with the most recent information available for maintaining an effective and trouble-free intelligence operations function. The course is designed specifically for those administrators who have the overall responsibility for directing a department to collect and maintain information on gangs, criminal extremist groups, terrorist organizations, and/or organized crime enterprises. For information, contact the Advanced Training Center at 916–464–1200 and ask for the program training officer or secretary for this course.

http://caag.state.ca.us/aticontent/criminal_intel.htm

UNIVERSITY PROGRAMS

Universities and colleges have programs or offer degrees in intelligence and related fields. For example:

California State University, Crime and Intelligence Analysis Certificate Program. The curriculum focuses on skill development in collecting and analyzing crime data to forecast future crime occurrences; developing target criminal profiles; documenting illicit relationships between people, organizations, and events; and using statistical techniques to solve crime problems. Participants are given practical instruction in crime analysis, criminal intelligence analysis, organized crime and intelligence analysis, and law enforcement research and statistical methods.

http://www.ccce.csus.edu/catalog/course_group_detail.asp?group_number=115&group_version=1

Mercyhurst College, Institute for Intelligence Studies. The Intelligence Studies Department offers a bachelor of arts degree in intelligence studies (formerly the Research Intelligence Analyst Program) and a master of science degree in applied intelligence. The undergraduate degree is designed to provide the necessary background for students to pursue careers in government and research or intelligence analysts in government agencies and private enterprise.

http://www.mculs.org/

Michigan State University, Criminal Justice Intelligence Program. This program will help law enforcement agencies develop and sustain a law enforcement investigative intelligence capacity in several ways by providing baseline information about and resource materials for the contemporary measuring and role of law enforcement intelligence; defining issues and pitfalls that may be encountered and providing guidance on how to prevent them; providing insight, understanding, and resources on intelligence trends; providing information about Federal law enforcement intelligence resources, processes, and products; and providing continuing education and technical assistance through the university’s School of Criminal Justice.

http://www.intellprogram.msu.edu/

BUREAU OF JUSTICE ASSISTANCE TRAINING

The following are courses of provided through the Bureau of Justice Assistance (BJA). BJA supports a broad array of training and technical assistance projects to strengthen the criminal justice system and public safety. Training organizations have received grants or contracts to provide training. Any State, tribal, or local agency or organization involved in activities related to fighting crime or ensuring public safety is invited to participate in training and technical assistance from BJA. For details and information on the following courses, visit BJA’s new training and technical assistance webpage.

http://www.ojp.usdoj.gov/BJA/ta/index.html

Cybercrime Investigation and Forensics

- Introduction to Internet Crime Investigations. This course introduces law enforcement investigators to the ways criminal activity is being perpetrated across online computer networks and teaches them in techniques for working these cases online.

- The Investigation of Computer Crime. This course teaches criminal justice investigators and support staff how to investigate high-technology theft and computer-related crime. It provides participants with an understanding of computer technology, its application to criminal endeavors, and the issues associated with investigating these cases.

- Seizure and Examination of Microcomputers. This class teaches criminal justice investigators the basic concepts of computers and digital evidence recovery. It teaches investigators new to high-technology crime how to safely seize a computer system, make duplicate images of hard drives, and recognize compressed and encrypted data; familiarization with forensic software; and the basics of digital evidence analysis.

- Investigation of Online Child Exploitation, Level I. This course is designed to provide law enforcement investigators and support staff with the skills necessary to conduct proactive Internet investigations involving child exploitation, such as how to initiate criminal investigations, establish undercover accounts and identities, and engage offenders legally and effectively. Topics include investigative software tools, undercover accounts, Internet culture and offender typology, record-keeping and case preparation techniques, network hardware and software, graphics and chat logs, online case investigations and process techniques, search warrants and raid issues, residual computer evidence issues and tools, and legal issues relating to child exploitation.

- Investigation of Online Child Exploitation, Level II. This course expands on the learning modules and fundamentals introduced in the Level I course and includes a detailed study of the Internet using America Online® (AOL) as an investigative tool. Topics include peer-to-peer investigations, desktop surveillance and advanced investigative resources, virtual child pornography that includes video enhancing and morphing, chat rooms and clubs, downloading and instant messaging software, instant messaging as a tool and an investigative resource, and sending information to newsgroups and Internet Relay Chat. (Continued)

- Advanced Internet Investigations. This intensive course is designed to improve law enforcement’s ability to successfully investigate and prosecute sophisticated crimes carried out over the Internet. Topics include the technical structure of the Internet, investigative methodology and tools, and audit logs as tools to protect online privacy issues, strategies for proper case preparation and presentation, host operating systems and system security, monitoring activity on an Internet host system, tracking suspects over the Internet, and other issues affecting the recovery of evidence from the Internet.

- Basic Local Area Network (LAN) Investigation. This 1-week course provides a basic understanding of computer networks. It provides the basic skills needed to investigate and solve crimes committed using a computer network, tips on where to look for evidence, and how to collect it in order to retrieve the evidence. On completion of this course, participants will have the skills necessary to properly seize a computer network and prepare it for forensic examination. The course includes an overview of the history of LANs/LAN architecture/equipment, investigative tools and techniques, peer-to-peer topology, hacking and network vulnerabilities, UNIX®/INT®/Novell® operating systems, and mandatory and examination of LANs, connecting networks together, and legal issues relating to LANs.

- Proactive Online Protection. This course offers training to school resource officers (SROs) and educators on Internet safety skills and on making highly effective, knowledgeable, and informative presentations to students on Internet safety issues. This course combines a review of several Internet safety programs with hands-on computer instruction and a curriculum that provides trainees with a working knowledge of what youth are often confronted with when accessing the Internet and online environments. It is recommended that the class contain a combination of SROs and educators who will provide the school presentations together.

Information Technology

- Compliance Training Seminar: 28 Code of Federal Regulations (CFR) Part 23. 28 CFR Part 23 is a guideline for law enforcement agencies that contains implementing standards for operating federally funded multijurisdictional criminal intelligence systems. It applies to systems operating through Federal funding under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended. BJA funds technical assistance and a half-day class that provides information on guidelines for operating criminal intelligence systems.

- Managing Criminal Justice Technologies in the 21st Century Seminar. This seminar is to help criminal justice executives and senior-level managers improve their capacity to deal with today’s technology while preparing for the challenges of the future. The educational goals include understanding the fundamental applications of computer and computer-related technologies, delineating methods to avoid and overcome pitfalls and problems associated with technology, and making appropriate decisions in the selection and purchase of computers and computer-based technologies for specific areas of the criminal justice system.

- Implementing Criminal Justice Technologies in the 21st Century Seminar. This seminar is for technology project managers and chief information officers who want to purchase software, hardw bake®/NT® ®

- The aim of this seminar is to help criminal justice executives and senior-level managers improve their capacity to deal with today’s technology while preparing for the challenges of the future. The educational goals include understanding the fundamental applications of computer and computer-related technologies, delineating methods to avoid and overcome pitfalls and problems associated with technology, and making appropriate decisions in the selection and purchase of computers and computer-based technologies for specific areas of the criminal justice system.

- Implementing Criminal Justice Technologies in the 21st Century Seminar. This seminar is for technology project managers and chief information officers who want to purchase software, hardw bake®/NT® ®
Justice Technology Training Series. The Technology Training Series is designed for managers and technical staff. The training agenda varies from basic introductions to a more indepth review of technical concepts and components. The technical training agendas can be tailored to the actual needs of the requesting agencies, both in terms of content and duration. Highlights of each agenda include the following:

- Information System Security Training. Participants will examine the unique challenges to making integrated criminal justice information systems secure and explore the technologies that contribute to a secure system. Information about best practices and “what works” in securing integrated justice projects, as well as administrative/management issues in implementing security protocols, will be presented.

- XML Training. Learn more about extensible mark-up language (XML), the costs and benefits of the technology, and how it can be used in an integrated justice environment. Instructors will provide applied exercises to help participants make sense of key concepts such as namespaces, schemas, and style sheets. Representatives from the vendor and practitioner communities will discuss nationwide initiatives, highlight XML, and talk about integrating justice projects at the State and local levels. The course is designed for technical and project personnel who are beginning to use XML. The course has two versions: The Basic XML Training Program serves as an overview of basic XML technical concepts and the Global Justice XML Data Model (GJXDM). It explains how XML and GJXDM are being used in the criminal justice environment. The Indepth XML Training Program has a deeper focus on GJXDM. This program serves as a good introduction to GJXDM and its technical concepts.

- Information Sharing and Data Mining Course. This course teaches participants how to use technologies and software approaches to create information out of data. Topics include how to use data warehouses, analytical software, and portal technology. It also contains presentations and demonstrations of actual systems in place that help make sense out of raw data and provide actionable intelligence.

- Web Services and Service-Oriented Architectures Course. This course teaches participants how to apply advanced concepts such as the GJXDM to actual systems through the use of Web services and the adoption of service-oriented architectures (SOA). It provides a basic introduction to the concepts of Web services and SOA. The course also includes a demonstration of how to build a Web service and explains the role of other standards such as Simple Object Access Protocol; Web Services Description Language; and Universal Description, Discovery, and Integration components. Lectures and exercises require some basic knowledge of information systems technology and understanding of XML.

- Road Map for Information Sharing Seminar. The UIS Institute and the National Criminal Justice Association offer a 16-hour seminar following on the highly successful past series of emerging technology for decisionmakers seminars. This new series is designed to help managers who are or may become involved in implementing information-sharing technology among law enforcement and criminal justice organizations increase the effectiveness of justice processes and provide greater homeland security. The seminar agenda is not a highly technical set of lectures for programmers, but a closely connected series of 11 sessions that explore useful aspects of information sharing in the justice community of interest. How-to demonstrations are for illustration purposes only and do not provide indepth training in the applicable skills of computer science or applications development.

- GJXDM Developer’s Workshops. In addition to the BJA-sponsored XML courses, the U.S. Department of Justice’s Office of Information Programs offers GJXDM Developer’s Workshops, sponsored and offered by partnering organizations at different locations throughout the country. GJXDM is being used across the Nation to enable law enforcement, court systems, corrections, and government agencies to share critical information in ways that save time and money. The workshops provide training on GJXDM version 3.0. Workshops are designed for developers and practitioners in the field. Since workshops are highly technical, an intermediate working knowledge of XML is recommended. For additional details and links to GJXDM-related training, workshops, meetings, and conferences, visit http://it.ojp.gov/topic.jsp?topic_id=110. GJXDM events also may be listed on the event calendar at http://it.ojp.gov/topic.jsp?topic_id=5. In conjunction with the workshops, GJXDM online training materials are available as a comprehensive educational resource, providing users with access to the workshop presentation slides, streaming video segments, answers to participant questions, program agenda, speaker information, technical documentation, practical exercises, and suggested solutions to in-class exercises. http://it.ojp.gov/topic.jsp?topic_id=116.

National Criminal Justice Reference Service

In addition to funding the National Law Enforcement and Corrections Technology Center, the National Institute of Justice (NJ) 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—

- JUSTINFO. A biweekly electronic news letter 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, 10 a.m. to 6 p.m. e.s.t.)
Fax: 301–519–5212
Mail: NCJRS, P.O. Box 6000, Rockville, MD 20849–6000

The National Law Enforcement and Corrections Technology Center is supported by Cooperative Agreement #2005–MU–CK–0077 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.

The U.S. Department of Justice, National Institute of Justice (NIJ), has released the Third Status Report to the Attorney General on Body Armor Safety Initiative Testing and Activities. Research results in the report show that Zylon®-containing used body armor may not provide the intended level of ballistic resistance. The results also indicate that a visual inspection of body armor and its ballistic panels is not sufficient to determine whether a particular piece of Zylon®-containing armor has maintained its ballistic performance.

Based on these findings, NIJ has issued an advisory notice listing poly-p-phenyleneterephthalamide (PPTA or Zylon®) as a material that appears to create a risk of death or serious injury in a result of degraded ballistic performance when used in body armor. NIJ has also adopted interim changes to its body armor compliance testing program that will ensure that officers are protected by body armor that maintains its ballistic performance during its entire warranty period.

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

Note: The mentioning of specific manufacturers or products in TECHshorts does not constitute the endorsement of the U.S. Department of Justice, National Institute of Justice, or the NLECTC system.
Tied up in technology?

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

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

Article Reproduction: Unless otherwise indicated, all articles appearing in TechBeat may be reproduced. We do, however, request that you include a statement of attribution, such as, “This article was reproduced from the Fall 2005 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 © 2005 Corbis Images; Getty Images; Veer; and Copshots.

Staff: Managing Editor, Rick Neimiller; Editor, Michele Coppola; Assistant Editor/Writer, Brian Higgins; Lead Writer, Becky Lewis; 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.
In the end it was a purple-colored computer disk mailed to a television station that cracked the case of BTK, the self-designated nickname used by Wichita, Kansas, serial killer Dennis Rader. Using technology to read “hidden” information contained on the disk, police were able to trace it back to a computer at a local church where Rader served as president of the council.

The information that led police to Rader is called “metadata.” And simply put, it’s data... about data.

In the cyberworld of home or office computers, metadata is information stored below the surface of documents, spreadsheets, and presentations created online through such office productivity suites as Microsoft® Office. Because this hidden data resides out of the visible interface, few users are aware that it is there. Metadata can contain personal information about the author of a file and the computer or network from which it was stored, saved, or printed. It can catalog e-mail addresses, the last 10 people who viewed the file, and/or past versions of the document. According to Salvatore Paladino from the National Institute of Justice’s CyberScience Laboratory in Rome, New York, the release of such metadata can be a starting point for hackers or divulge sensitive information to those who should not have it. The improper release of metadata has caused embarrassment, resulted in the loss of intellectual property, influenced the outcome of legal proceedings, and even endangered lives.

When controlled properly, however, corporate security professionals and computer forensic investigators can use metadata to investigate, for example, an employee who is suspected of accessing a document without proper authorization, to establish a link between two suspects, or to uncover a valuable piece of the investigative puzzle.

An awareness of metadata will not only protect an organization, but also provide investigators with the ability to reveal hidden data lurking in electronic evidence. This makes it imperative that investigators be able to locate, identify, uncover, and remove metadata as needed.

To obtain a technical report that describes metadata in greater detail, go to www.cybersciencelab.com. (Registration on the Private Site is required to complete the download.) For more information about metadata training resources, contact Salvatore Paladino, 888-338-6584 or salvatore.paladino@rl.af.mil.