U.S. Department of Justice Office of Justice Programs *National Institute of Justice*



NIJ

National Institute of Justice **JOURNAL**



Body Armor Safety Initiative: To Protect and Serve...Better

by Dan Tompkins

Analyzing Terror: Researchers Study the Perpetrators and the Effects of Suicide Terrorism *by Michael S. Hronick*

Keeping an Eye on School Security: The Iris Recognition Project in New Jersey Schools *by Jeffrey P. Cohn*

Maximize Your Evaluation Dollars by Edwin Zedlewski with Mary B. Murphy

Digital Evidence: How Law Enforcement Can Level the Playing Field With Criminals by Nancy Ritter

Methamphetamine Abuse: Challenges for Law Enforcement and Communities by Dana E. Hunt

Has Rape Reporting Increased Over Time? *by Lauren R. Taylor*

U.S. Department of Justice Office of Justice Programs

810 Seventh Street, N.W.

Washington, DC 20531

Alberto R. Gonzales Attorney General

Regina B. Schofield Assistant Attorney General

Glenn R. Schmitt Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

National Institute of Justice www.ojp.usdoj.gov/nij

Office of Justice Programs Partnerships for Safer Communities www.ojp.usdoj.gov

JR 000254

2006

ISSUE NO. 254

DIRECTOR'S MESSAGE

In the early 1970s, one of NIJ's staff had a "eureka" moment. He wondered if a new material called Kevlar, principally used in car tires, might work as a type of armor to protect police officers. Working with a colleague from the Defense Department, they convinced NIJ and DoD to work together to test out the idea.

By 1975, work on the project had progressed to the point where the material worked in controlled tests. Now it was time to field-test it. That summer, 5,000 prototype bullet-resistant vests, relatively soft and lightweight, were distributed to 15 urban police departments. But researchers knew what the next logical step was—analyzing the performance of a vest involved in an actual police shooting. And that meant that someone had to get shot while wearing one.

The uneasy vigil ended on the evening of December 23, 1975, when one of the vests stopped bullets fired at a Seattle police officer—and saved his life. And with that event NIJ claimed the first in a line of successes from its body armor standards and testing program—more than 3,000 police officer lives saved.

This issue of the *NIJ Journal* features an article describing NIJ's body armor program on its 30th anniversary and summarizing a critical review of the program currently underway as part of the Attorney General's Body Armor Safety Initiative.

This issue also explores how recent advances in another technology—biometrics can protect people, in this case schoolchildren. NIJ recently sponsored a program evaluating iris-recognition technology in a New Jersey elementary school. Researchers evaluated how effectively the technology could identify the teachers, parents, and other adults who were supposed to be there—and keep out those who were not.

But technology can cut both ways. Just as law enforcement uses technology to prevent or investigate crime, perpetrators use technology to commit crime. Often, State and local police departments must scramble to keep up. To help them, NIJ sponsors the Electronic Crimes Partnership Initiative (ECPI), a group of law enforcement practitioners who train police officers to investigate and solve computer crimes and to search for and collect digital evidence in criminal investigations. Their work is featured in "How Law Enforcement Can Level the Playing Field With Criminals."

In response to the global rise of suicide terrorism, NIJ convened an international panel of specialists to discuss how to use research to understand the dynamics of this troubling phenomenon, to combat its use, and to mitigate its effects. You can read a summary of that conference in this edition.

The articles in this issue of the *NIJ Journal* exemplify the wide-ranging scope of NIJ's research, development, and evaluation activities—and the dedication and creativity of its employees—in pursuit of an improved criminal justice system. I hope you will find something of interest in the pages that follow.

Hom R. Schmith

Glenn R. Schmitt Acting Director, National Institute of Justice



2006

JULY 2006

Contents

Features

Body Armor Safety Initiative: To Protect and Serve Better by Dan Tompkins	2
Analyzing Terror: Researchers Study the Perpetrators and the Effects of Suicide Terrorism by Michael S. Hronick	8
Keeping an Eye on School Security: The Iris Recognition Project in New Jersey Schools by Jeffrey P. Cohn	12
Maximize Your Evaluation Dollars by Edwin Zedlewski with Mary B. Murphy	16
Digital Evidence: How Law Enforcement Can Level the Playing Field With Criminals by Nancy Ritter	20
Methamphetamine Abuse: Challenges for Law Enforcement and Communities by Dana E. Hunt	24
Has Rape Reporting Increased Over Time? by Lauren R. Taylor	28
Also in This Issue	
Publications of Interest From NIJ	7

NIJ and Harvard University Webcast Addresses Prisoner Reentry 23

Keeping You Up-to-Date

For the latest NIJ news and time-sensitive information, visit the NIJ Web site at www.ojp.usdoj.gov/nij and click on 'What's New.' Here you'll find the latest information about NIJ publications, solicitations, conferences, and career opportunities.

Be sure to visit often-it's updated regularly!



Body Armor Safety Initiative: To Protect and Serve...Better by Dan Tompkins

About the Author

Dan Tompkins is a writer/editor at the National Institute of Justice and Editor of the *NIJ Journal*.

n December 23, 1975, Seattle Police Department Patrolman Raymond T. Johnson stood in the checkout line at a local market when a robbery suspect entered the store and brandished a weapon. Johnson lunged for the suspect's gun. In the violent struggle that ensued, the suspect emptied his .38 caliber pistol, striking Johnson in the left hand and twice in the chest before fleeing.¹ Johnson survived with severe hand injuries, chest bruises, and a unique distinction—the first law enforcement officer saved in a field test of a new generation of soft body armor being conducted by the National Institute of Justice (NIJ).

Johnson was wearing body armor made with Kevlar[®], an extraordinarily strong fabric developed by DuPont. NIJ, in partnership with the U.S. Army, began a program in the early 1970s to develop lightweight body armor woven from Kevlar[®]. Field testing began in the summer of 1975, with 5,000 armors provided to 15 urban police departments. Less than 6 months later, Johnson was the first officer saved by one of the field test armors. In all, 17 other armor-wearing officers were saved during the 1-year field test.

About the same time, NIJ developed a performance standard for body armor in collaboration with the National Institute of Standards and Technology (NIST, then known as the National Bureau of Standards),² followed by a voluntary testing program. The standards and testing program, which still exists today, enables body armor manufacturers to certify the performance and safety of new body armor.³ The NIJ standard establishes minimum performance requirements for armor, and the testing program evaluates armor against the standard.

Twenty-eight years later, on the night of June 23, 2003, Forest Hills, Pennsylvania, Police Officer Edward Limbacher, wearing body armor constructed primarily of a fiber

called Zylon[®], threw open the side door of an unmarked Econoline van and stepped out to move in on a drug suspect. The suspect fired, striking Limbacher in the arm and abdomen with .40 caliber rounds. The shot to the abdomen penetrated the body armor Limbacher was wearing. He survived but sustained severe injuries.⁴

The Forest Hills shooting was the first case ever reported to NIJ in which body armor compliant with the NIJ standard failed to prevent penetration from a bullet it was designed to defeat.

In the 28 years between those two incidents and in the time since, at least 3,000 officers survived shootings or other incidents because they were wearing body armor meeting NIJ performance standards.⁵ But the Forest Hills incident caused great concern within the law enforcement community and within the U.S. Department of Justice: Are we keeping our officers safe?

The Body Armor Safety Initiative

In November 2003, in the aftermath of the Forest Hills incident, then Attorney General John Ashcroft announced a Body Armor Safety Initiative to address the reliability of body armor used by law enforcement and to review the process by which body armor is certified.⁶

As part of the initiative, NIJ tested both new and used ballistic-resistant vests made with Zylon^{®, 7} NIJ also tested upgrade kits distributed by the manufacturer of the armor in the Forest Hills incident to retrofit some models of its Zylon[®]-based vests. And NIJ began a review of its standards and testing program for ballistic-resistant vests, which has resulted in interim changes to the standards and testing process. Read on for the results of these tests and a summary of changes to the standards and testing program.

Why Did the Vest Fail?

Even before the announcement of the Attorney General's initiative, NIJ staff contacted representatives of the Forest Hills Police Department and the Allegheny County Police Department (the agency handling the criminal investigation of the shooting) to examine the vest, the weapon, and the ammunition used in the shooting to determine why the vest failed. The examination found that:

- The bullet velocity from the gun used in the shooting was not greater than the bullet velocity NIJ uses in compliance testing for the type of vest Limbacher was wearing.
- The physical properties of the bullets used in the shooting were similar to bullets used in NIJ's compliance testing of the type of vest Limbacher was wearing, although there were some differences in bullet geometry and in how the bullet deformed on impact.
- The tensile strength of Zylon[®] yarns removed from the back panel of Limbacher's vest was up to 30 percent lower than Zylon[®] yarns from new armor that the manufacturer provided for this study. (The front panel, which was penetrated in the incident, was being held as evidence in the criminal case against the shooter, so it was not available for testing.)

NIJ also developed a detailed test plan simulating the Forest Hills incident to isolate the factors deemed most likely responsible for the vest failure. Test designers identified five potential causal factors: ballistic material tensile strength, bullet type, the gun barrel twist, the shot angle, and the location of the shot on the armor.

NIJ obtained and tested 32 ballistic panels of the type worn in the Forest Hills incident. Half of the panels were tested new, and the other half were artificially aged for 5 months in a chamber exposing the panels to controlled temperature and humidity conditions until the tensile strength of fibers in the vests matched those of fibers from the rear panel of the Forest Hills vest.

Each of the 32 panels was shot six times. None of the 192 shots penetrated the panels. NIJ is continuing efforts to determine the cause of the Forest Hills failure but is still unable to draw a definitive conclusion.

Testers found no correlation between the level of visible wear of the body armor panels and the ballistic performance of those panels. This finding is important because even used Zylon[®] body armor that appears to be in good condition may not provide an acceptable level of performance.

Testing the Upgrade Kits

As part of the Attorney General's initiative, NIJ was directed to test any upgrade kits offered by body armor manufacturers to retrofit existing vests. The tests would determine if the upgrade kits met the NIJ performance standard when used with the original vest they were designed to supplement. One manufacturer, Second Chance Body Armor, Inc. (the manufacturer of the body armor worn in the Forest Hills incident), offered an upgrade kit to users of some models of Zylon[®]-based body armor-an additional ballistic panel to be inserted into the armor. At NIJ's request, Second Chance provided 50 sets of armors and matching upgrade kits for three soft armor protection levels-Level IIA, Level II, and Level IIIA.⁸ The samples included both new and used upgrade kits, and the majority of the armors had been previously worn.

NIJ's testing found that the Second Chance upgrade kits added protection when used with the existing used body armor. However, the level of protection did not meet existing NIJ performance standards for new body armor.

Also, the vest/upgrade kit combinations in all three protection levels experienced excessive "backface signatures." This means that the bullets didn't penetrate the vest, but the impact of one or more bullets created a "dent" of more than 44 mm (almost 2 inches) into the clay in back of the vests during testing, a depth that may cause serious injury. Six of eight Level IIA armors, two of eight Level II armors, and five of eight Level IIIA armors ultimately tested experienced excessive backface signatures during testing.

Further, two of the eight Level IIIA vest/ upgrade kits (designed to offer protection against high velocity 9 mm and 44 magnum bullets) experienced penetrations.

Despite the safety questions raised by these test results, it is important to note that the upgrade kits did add some measure of protection. Officers who have received these upgrade kits should wear them.

Testing Used Armor

Heat, moisture, ultraviolet and visible light, detergents, friction, and stretching may all contribute to the degradation of fibers used in the manufacture of body armor. Body armor manufacturers design their armor and provide care instructions to minimize the effects of these degrading properties.

Because the evidence showed an unexpected degradation rate in Zylon[®]-based armor, NIJ conducted ballistic and mechanical properties testing on 103 additional used body armors containing Zylon[®]. Law enforcement agencies across the United States provided these vests to NIJ. Sixty of these used armors (58 percent) were penetrated by at least one round during a six-shot test series. Of the armors that were not penetrated, 91 percent had backface deformations in excess of that allowed by the NIJ standard for new armor. Only four of the used Zylon[®]-containing armors met all performance criteria expected under the NIJ standard for new body armor compliance. Although these results do not conclusively prove that all Zylon[®]-containing body armor models have performance problems, the results show that used Zylon[®]-containing body armor may not provide the intended level of ballistic resistance.

In addition, armors were visually inspected and given one of four condition ratings from "no visible signs of wear" to "extreme wear and abuse." Testers found no correlation between the level of visible wear of the body armor panels and the ballistic performance of those panels. This finding is important because even used Zylon[®] body armor that appears to be in good condition may not provide an acceptable level of performance.

Exploring Fiber Degradation

With funding provided by NIJ, polymer scientists at NIST are probing down to the molecular level to learn more about how Zylon[®] degrades. They are examining the chemical changes that occur as the fibers degrade, the trace contaminants on fibers that may contribute to degradation, the moisture content of fibers, and mechanical strength differences among individual fibers and what causes those differences.

Initial findings have isolated the ballistic performance degradation to the breakage of a small part of the Zylon[®] fiber molecule. Breakage of this part of the molecule, called the oxazole ring, occurs as a result of exposure to both moisture and light. When there was no potential for external moisture to contact Zylon[®] yarns, there was no significant change in the tensile strength of these yarns. Therefore, it appears that external moisture is necessary to facilitate the degradation of Zylon[®] fibers.

In addition to this work, NIJ is also funding research on other personal protective equipment to better understand how and why ballistic-resistant materials degrade over time.⁹

Improving the NIJ Standard and Compliance Testing Program

NIJ has undertaken a complete review of its performance standard for ballisticresistant armor and the compliance testing program. It solicited input from law enforcement and corrections agencies, fiber and armor manufacturers, and standards and testing organizations. *The evidence is clear: An officer not wearing armor is 14 times more likely to suffer a fatal injury than an officer who is.*

NIJ's 2005 Interim Requirements for Bullet-Resistant Body Armor, issued in August 2005, take into account the possibility of ballistic performance degradation over time. These interim requirements will help ensure that officers are protected by body armor that maintains its ballistic performance during its entire warranty period.

Under the 2005 interim requirements, NIJ will not deem armor models containing PBO (the chemical basis of Zylon[®]) to be compliant unless their manufacturers provide satisfactory evidence to NIJ that the models will maintain their ballistic performance over their declared warranty period.

NIJ recommends that agencies that purchase new ballistic-resistant body armor select body armor models that comply with the NIJ 2005 Interim Requirements. A list of models that comply with the requirements is maintained at www.justnet.org/BatPro.

NIJ is also encouraging manufacturers to adopt a quality management system to ensure the consistent construction and performance of NIJ-compliant armor over its warranty period. In the future, NIJ will issue advisories regarding body armor materials that appear to create a risk of death or serious injury as a result of degraded ballistic performance. Any body armor model that contains any material listed in such an advisory will be deemed no longer compliant with the NIJ standard unless the manufacturer satisfies NIJ that the model will maintain ballistic performance over the declared warranty period.

Life Vests

There are at least 3,000 other stories like that of Seattle Police Officer Raymond T. Johnson. That's 3,000 families spared the anguish of death or debilitating injury to a loved one in the line of duty. And cases like that of Forest Hills Officer Limbacher's are rare—a testament to the reliability of soft body armor. Even so, that single failure prompted NIJ to review its body armor program and to conduct an intensive examination of why that failure occurred. Through this review and research, NIJ remains committed to working for the safety of law enforcement officers.

The evidence is clear: An officer not wearing armor is 14 times more likely to suffer a fatal injury than an officer who is. Therefore, the most important message for the law enforcement community is that officers should continue to wear their body armor.

At least 3,000 officers would second that advice.

NCJ 214112

For More Information

Status reports on the Attorney General's Body Armor Safety Initiative and other updates on the activities in support of the Initiative are posted on the Bulletproof Vest Partnership/Body Armor Safety Initiative Web site at www.ojp.usdoj. gov/bvpbasi.

Notes

 The suspect was arrested 6 weeks later and charged with first-degree assault and attempted robbery. He was convicted and sentenced to 15 to 30 years' imprisonment.

- 2. Commercial body armor was being manufactured and sold even as NIJ's field test began, accelerating the need for a standards program. In fact, the first documented "save" unrelated to NIJ's field test occurred in May 1973 in Detroit, Michigan.
- 3. More information about NIJ's body armor standards and testing program can be found at NIJ's National Law Enforcement and Corrections Technology Center Web site, JUSTNET, at www.justnet.org/testing/ bodyarmor.html.
- 4. The suspect fled but was arrested later that night. In April 2004, he was convicted of 2 counts of attempted homicide, 11 counts of aggravated assault, and 9 counts of reckless endangerment related to the June 23, 2003, incident.
- 5. In 1987, DuPont and the International Association of Chiefs of Police (IACP) created the Kevlar Survivor's Club, which recognizes law enforcement and corrections officers who survive life-threatening or disabling events because they were wearing personal protective body armor. In March 2006, IACP commemorated Atlanta Police Department Officer Corey B. Grogan as the 3,000th documented save. A Web site, www.dupont.com/ kevlar/lifeprotection/survivors.html, keeps a tally of survivors, maintains a database of survivor stories, and provides criteria and instructions for membership.
- A Web site supporting the Body Armor Safety Initiative is located at www.ojp.usdoj. gov/bvpbasi.
- 7. Zylon fiber is manufactured by Toyobo Co., Ltd., of Japan.
- For a description of the protection levels, see NIJ's Ballistic Resistance of Personal Body Armor, NIJ Standard-0101.04, www.ojp.usdoj.gov/nij/pubs-sum/183651.htm.
- 9. The most recent NIJ solicitation for concept papers, "Officer Safety Equipment," is available at www.ncjrs.org/pdffiles1/ nij/sl000720.pdf.

M

3

NIJ

NL

Publications of Interest From NIJ

Public Law 280 and Law Enforcement in Indian Country: Research Priorities

Passed in 1953, Public Law 280 (PL 280) gave jurisdiction over criminal offenses involving Indians in Indian country to certain States and allowed other States to assume jurisdiction. Subsequent legislation allowed States to retrocede jurisdiction, which has occurred in some areas. This Research in Brief summarizes the current status of PL 280 jurisdiction, identifies the key issues, and lists areas for further research and action.

Available at www.ncjrs.gov/pdffiles1/ nij/209839.pdf.

Juvenile Accountability Incentive Block Grants: Assessing Initial Implementation

Congress created Juvenile Accountability Incentive Block Grants (JAIBG) in 1997 to encourage States and localities to strengthen prosecution and adjudication of juvenile offenders. The Office of Juvenile Justice and Delinquency Prevention began awarding JAIBG funds in 1998. The National Institute of Justice authorized Abt Associates Inc. to conduct a process evaluation to determine how block grant funds were spent in the initial years of the grant and how States and localities conformed to policy objectives envisioned by Congress. This Research for Policy, based on a more extensive final report to NIJ, discusses the key evaluation findings.

Available at www.ncjrs.gov/pdffiles1/ nij/210116.pdf.

Co-Offending and Patterns of Juvenile Crime

Juveniles often commit crimes in pairs or groups, which is known as cooffending. Results of an NIJ-sponsored study of delinquents in Philadelphia showed that co-offending is linked to increased risks for recidivism and violence, and interaction among delinquent peers seems to instigate crimes and escalate their severity. The researchers recommend early intervention targeting very young offenders, especially co-offenders. But they also caution that some interventions may enhance the effects of co-offending by placing youths in groups that unintentionally provide negative peer learning.

Available at www.ncjrs.gov/ pdffiles1/nij/210360.pdf.

Sexual Assault on Campus: What Colleges and Universities Are Doing About It

College women are at higher risk for sexual assault than their non-college-bound peers. Yet, many rapes and attempted rapes are unreported, perhaps because for the majority of these crimes, the victim and assailant are acquainted. Schools vary widely in how they comply with Federal requirements to report and respond to sexual victimization. These are among the findings from the first major survey of the Nation's colleges and universities inquiring about sexual assault on campus and how schools report and handle the problem. Many schools need guidance on how to comply with Federal requirements to disclose security procedures, report crime data, and ensure victims' rights. Promising practices in prevention, policy, victim support services, and other areas are discussed.

Available at www.ncjrs.gov/pdffiles1/ nij/205521.pdf.

Enhancing Police Integrity

What factors contribute to or detract from police officer integrity, and how can police administrators measure integrity? A national survey of police officers identified characteristics of agency culture that encourage officers to resist or tolerate certain types of misconduct. This Research for Practice summarizes the survey findings and includes an assessment tool that police chiefs can use to measure integrity within their departments.

Available at www.ncjrs.gov/pdffiles1/ nij/209269.pdf. NL



Analyzing Terror: Researchers Study the Perpetrators and the Effects of Suicide Terrorism

by Michael S. Hronick

About the Author

Michael S. Hronick is a Social Science Analyst with the International Center of the National Institute of Justice.

S ince September 11, 2001, research on terrorism has increasingly focused on suicide terrorism. Though the number of terrorist attacks has decreased since the mid-1980's,¹ fatalities have dramatically increased because of a rise in especially lethal suicide attacks by individuals on behalf of terrorist organizations.²

NIJ hosted a Suicide Terrorism Research Conference in October 2004 that brought together a distinguished panel focused on this phenomenon. (See "Conference Presenters.") Although the presenters differed in their approach to the study of suicide terrorism, the discussions yielded a rich exchange of ideas that may serve to broaden the scope of future research.

Existing Research on Suicide Terrorism

Allison Smith of the American Association for the Advancement of Science (then a fellow with the Department of Homeland Security) reviewed 34 research projects on suicide terrorism. Most of the projects reviewed were released in 2002 or later. She categorized the different research methods to study suicide terrorism: expert analysis (37 percent), interviews (20 percent), literature reviews (14 percent), analysis of event datasets (14 percent), data from secondary sources, including legal proceedings and articles (9 percent), and surveys (6 percent).

Smith also summarized the recommendations made by the 34 projects. The most common recommendations (and the frequency with which they were recommended) included:

"Weaken terrorist groups by targeting leaders." (6)

- "Realize that attacking groups may lead them to become more adaptive and/or ruthless." (6)
- "Develop informants to infiltrate terrorist groups." (5)
- "Strip away the terrorist groups' supporters by engaging them in dialogue." (5)

What Is "Suicide Terrorism"?

Clear operational definitions and well-defined variables are a challenge to researchers who study suicide terrorism. Some conference attendees disagreed on which definition of suicide terrorism to use.

Andrew Silke of the University of East London noted that throughout history, acts that some might dismiss as "crazy" or "diabolical" have frequently been employed as rational terrorist tactics. Examples include Cato's self-inflicted stabbing and Samson's destruction of the temple where he was held. He noted that groups that have used suicide as a tool include Japanese samurai, English suffragists, IRA hunger-strikers, and Japanese kamikaze pilots. Silke also raised the question of how we should consider last-stand battles, such as the Spartans at Thermopylae or Americans at the Alamo. Silke's historical framework prompted the panel of experts to debate how best to determine the difference between suicide and "suicidal" (high-risk) acts. Central to the discussion was deciding whether an act that is considered suicidal contributes seminal knowledge to the understanding of suicide terrorism. In other words, should the definition of suicide terrorism be limited to actions that result only in suicide or should suicidal acts be included as well?

Ariel Merari of Tel Aviv University thought some terrorist acts were deviations from the true act of suicide terrorism. Merari distinguished suicide terrorism as "intentionally killing oneself for the purpose of killing others, in the service of a political or ideological goal" and discounted "highrisk missions, fooled couriers, and suicide without homicide for a political cause" from suicide terrorism research. There is a great psychological difference between killing oneself intentionally and undertaking a mission with a high risk of death, according to Merari. A large proportion of terrorist attacks involve some risk of death for the perpetrators. However, with the exception of true suicide attacks, researchers cannot assess the objective and subjective chance of death. Thus, expanding the definition of suicide attacks to include high-risk missions would contaminate the sample and make it impossible to construct a generally accepted list of suicide attacks.³

Psychological Autopsies

The psyche of the suicide terrorist prompted considerable discussion. Participants generally concurred that perpetrators are mislabeled as "mentally unstable." They may possess weaker personalities, but they are almost exclusively sane and even logical.⁴ These conclusions result in part from a research method known as the "psychological autopsy." Arjuna Gunawardena of Protecht Risk Management Solutions, Ltd. explained the psychological autopsy, one of the research techniques pioneered by Merari in his study of suicide terrorism in Israel, and used by Gunawardena in his study of the Black Tiger suicide cadres of the LTTE in Sri Lanka. This deductive, investigative research method attempts to reconstruct the psyche of the perpetrator based on interviews, records, communiqués, and other imprints of the individual.

Mohammed Hafez of the University of Missouri-Kansas City stated that suicide attacks are often conducted by secular organizations to advance political objectives against a stronger, technologically superior enemy. He noted that these organizations often invoke religion to appeal to individuals in order to convince them that they are fulfilling a commitment to God.

Hafez also explained how what he called the "reward of martyrdom" might motivate an individual to undertake a suicide attack and cited terrorists in Palestinian society as an example. There, suicide attackers are regarded by some as heroes, with their names given to babies or streets, and their sacrifices promoted by posters and mass funerals. Among the purported rewards

Conference Presenters

- Dr. Andrew Silke, University of East London.
- Dr. Allison Smith, American Association for the Advancement of Science (then a fellow with the U.S. Department of Homeland Security).
- Mr. Arjuna Gunawardena, Protecht Risk Management Solutions, Ltd., Sri Lanka.
- Dr. Mohammed Hafez, University of Missouri-Kansas City.
- Dr. Ariel Merari, Tel Aviv University.
- Ms. Nasra Hassan, United Nations Office on Drugs and Crime, Austria.
- Dr. Marc Sageman, University of Pennsylvania.
- Dr. Robert Pape, University of Chicago.

Also present at the conference were staff from:

- White House Office of Science and Technology Policy.
- U.S. Department of Homeland Security.
- Israeli Ministry of Public Security.
- U.S. Department of Defense.
- National Institutes of Health.
- Federal Bureau of Investigation.
- Representatives of other government and national security agencies.

Participants generally concurred that perpetrators are mislabeled as "mentally unstable." They may possess weaker personalities, but they are almost exclusively sane and even logical. for a martyr in the afterlife are the ability to intercede with God on behalf of friends and family and redemption for not only the individual, but for the society as well. Also, organizations that sponsor terrorism often bestow money and status on the families of suicide terrorists.

Merari's assertion that suicide terrorists are not religious fanatics supported the discussion among other attendees that religion plays a tertiary role to organizational pressure and political goals.

Merari's research isolated several personality traits typical of suicide attackers. They possess weak personalities; are socially marginalized; are subject to rigid, concrete thinking; and demonstrate low self-esteem. He reported the four motivating factors often cited by suicide attackers: national humiliation, religion ("to do God's Will"), personal revenge, and admittance to paradise in the afterlife.

Merari and others emphasized the influence of the group over individuals in planning suicide attacks. Following recruitment into a terrorist organization, individuals make a commitment to the group in the form of a contract, which leads to a personal commitment to the mission.

Marc Sageman of the University of Pennsylvania described a typical scenario by which a person becomes a terrorist through the vehicle of religion. A socially aloof individual, perhaps new to the area, joins others at a place of worship. After meeting similar individuals there (a "bunch of guys," in Sageman's words), they begin to socialize. Initially, they convene to share a common faith and similar interests, but later, their association assumes an increasingly radical essence. At this point, attachment to the group ("in-group love") trumps other considerations and affects perceptions ("out-group hate"), and the individual feels obligated to participate in terrorist activity out of loyalty to the group. It is these groups that heed the summons to "kill the infidels" or to join the "global Salafi⁵ jihad" by al Qaeda.

Moving Forward

Participants widely agreed with the assertion by Robert Pape of the University of Chicago that researchers must have access to each other's data in order to gain multiple perspectives on terrorist incidents and to mine those data for future research. He recommended that a central terrorism database be created.

Pape's desire for a centralized, comprehensive database is a byproduct of his studies. He began his research on suicide terrorism following the attacks of 9-11 and discovered that aggregate data on the subject were not available prior to the year 2000. In response, he gathered data from a variety of sources. He found that 95 percent of the suicide terrorist attacks conducted since 1983 could be categorized into clusters, or "campaigns." He theorized that the efficacy of these campaigns has led to an increasing reliance on suicide attacks as a tactic to effect a political outcome. Pape observed 16 separate campaigns from 1983 to 2005, 4 of which are ongoing. In most, the target was a democracy with an occupying military presence.

At the conclusion of the conference, participants were asked to offer their insights on suicide terrorism and what measures should be taken in the future. Some of the suggestions included:

- Research efforts should yield practical results for practitioners combating suicide terrorism and should focus on three areas:

 the launching of the attack, 2) identifying characteristics of the bombers onsite with the aim of stopping them, and
 having failed that, minimizing injury and other harm to victims by shielding them and empowering the general population by building up their psychological resilience (Israel L. Barak-Glantz, Ministry of Public Security, Israel).
- Researchers should analyze information about terrorist groups available on the Internet and in publications, which are often provided by the groups themselves (Peter Probst, Institute for the Study of Terrorism and Political Violence, United States).

- Several questions in need of more analysis include: 1) What can we learn from failed attempts by suicide bombers? 2) What are the profiles of the leaders of movements that promote suicide operations? 3) How do we minimize the psychological effects of terrorism in general, and suicide terrorism in particular? 4) What is the impact of the cult of suicide terrorism on the societies that encourage acts of martyrdom? (Joshua Sinai, Program Manager, Terrorism Studies, Logo Technologies, United States, formerly with the Department of Homeland Security).
- Future research should focus on:

 situations conducive to suicide bombing, 2) characteristics of groups and their decision-making processes,
 methods of recruiting and training bombers, 4) personality factors of and social influences on suicide terrorists (a comparative study of universal characteristics), 5) the effect of government responses, and 6) the effects on the target (Ariel Merari, Tel Aviv University, Israel).
- The phrase "suicide bomber" must not be used interchangeably with the phrase "suicide terrorist." Other methods of suicide attack are not aptly described by the term suicide bomber (Carole Murti, U.S. Department of Defense, United States).

The panelists accepted two administrative points as critical for productive future research in this field: 1) the need for suicide terrorism researchers to share their data, and 2) the need for researchers to acknowledge differences in the operational definition of suicide terrorism and to explicitly state their working definition as part of any reporting of research findings.

NIJ's conference was a forum for researchers studying what has become a deadly trend. The meeting offered an opportunity for experts in the field to present their findings, exchange ideas, and return to their respective organizations and institutions with the benefit of the perspectives, successes, and failures of the research conducted by their peers throughout the world. NIJ remains committed to fostering this interaction and to supporting terrorism research that will impact policy and practice—one step toward alleviating the threat to the safety of the world's people and the rule of law.

NCJ 214113

Notes

- Terrorist acts peaked in 1987 with 666 incidents. A low of 274 attacks was recorded in 1998. There were 348 attacks reported in 2001 (presentation by Pape, Robert, NIJ, October 2004), 175 attacks reported in 2003, and 651 attacks recorded in 2004. However, 2004 data were collected using a different method. The National Counterterrorism Center cautions against comparing the 2004 figures with previous data due to this new method ("Global Terrorism Statistics Released," *The Washington Post*, April 28, 2005, A07).
- Suicide attacks have increased from 31 in the 1980's to 104 in the 1990's to 53 in 2001 alone. The number of victims has increased as well, from approximately 700 fatalities in the 1980's to more than 3,000 in 2001. To view statistical charts, see Pape, Robert, "The Strategic Logic of Suicide Terrorism," *American Political Science Review*, 97(3) (August 2003): 1–19. Statistics on terrorism trends are also available from the U.S. Department of State at www.state.gov/s/ct/ rls/pgtrpt.
- 3. The delegation from the Israeli Ministry of Security was very firm on this point. Members felt that a very specific mindset is needed to carry out a suicide bombing. To analyze anyone other than one who, with the exception of a mechanical failure or thwarted attempt, has a successful mission is detrimental to understanding the causes and realities of this tactic.
- 4. Silke, Merari, and Sageman each made a point of dispelling any concept of suicide attackers as mentally unstable.
- 5. The term salafi is a derivative of the word salaf, which is a reference to the Prophet Mohammed and his companions. Modern, radical Muslims (Salafists) advocate a return to the glory years of Islam (c. 622 A.D. to 662 A.D.), often resulting in calls for jihad. They feel that, in order to transform Muslim states that have fallen astray (by becoming more Westernized or more corrupted), they must be more like the Muslim states of that golden age. Leaders such as Osama bin Laden call for destruction of the "far-enemies," such as the United States, prior to battling the "near-enemies," such as the leaders of modern Muslim states. This demand is answered on an international scale by al Qaeda adherents.



Keeping an Eye on School Security: The Iris Recognition Project in New Jersey Schools by Jeffrey P. Cohn

About the Author

Jeffrey P. Cohn is a freelance writer/reporter.

ow can school administrators, teachers, staff, and parents make their schools safe for adults and children alike? How do you let parents and other authorized individuals into the building while keeping unauthorized people out without using up staff time to check identities and permissions? How do you know that a person entering a school building is who he or she claims to be? And how do schools resolve these questions without invading someone's personal privacy?

One way involves a security system that links eye-scanning cameras with computers to identify people who have been preauthorized to enter the schools and then, once their identity is confirmed, lets them in by unlocking the door. The system has been adopted by three Plumsted Township schools in New Egypt, New Jersey, under a \$293,000 science and technology grant from the National Institute of Justice. More recently, NIJ awarded a second grant to install a similar eye-scanning system in another, more demographically diverse New Jersey school.

In addition, NIJ funded an evaluation of the field test of the technology in the New Egypt schools. 21st Century Solutions, Inc. conducted an independent evaluation of the project, working in partnership with the schools and NIJ.

Nicknamed T-PASS (an acronym for Teacher-Parent Authorization Security System), the system in New Egypt identifies people using cameras that focus on 240 separate points on their irises. The iris is the round, pigmented area surrounding the pupil that controls how much light enters the eye. The experimental system represents the first use of iris recognition technology as a security measure for schools in the United States. Elsewhere, iris scanners are used to track inmate movements inside a dozen or so U.S.

jails and to ensure that any prisoners being released are indeed the right ones. They are also used to identify some people entering Canada from the United States; some airline passengers at Reagan National Airport in Washington, DC, and other U.S. airports; and ATM users in Great Britain.

The ABCs of Biometrics

The use of iris scanners falls under what scientists and engineers call "biometrics." Biometrics refers to a variety of computerbased technologies for recognizing individuals and verifying their identities using one or more of their physiological and/or behavioral characteristics. It has the distinct advantage of not requiring us to remember a user name, password, or series of numbers while confirming that we are who we claim to be. Biometrics is more reliable than traditional identifiers, such as driver's licenses and identification or swipe cards, because it relies on individually unique characteristics. And because it is tied to a computer, biometrics is fast and provides a record that other methods usually do not.

Biometrics systems can use one or more of several different physical and/or behavioral characteristics for identification and verification. These include iris, retinal, and facial recognition; hand and finger geometry; fingerprint and voice identification; and dynamic signature. Some methods, like iris scans, are more technologically and commercially advanced than others. Which biometric method works best varies significantly from one application to another and even from one vendor to another. It depends on how and for what purpose the system is to be used; the level of accuracy and reliability required; and such factors as cost, speed, and user acceptance. None provides 100 percent accuracy.

Whatever method is used, biometrics basically involves a three-step process. First, a camera, scanner, or other sensor takes an image or picture. Second, that image is made into a pattern known as a biometric signature. Third, the biometric signature is converted into a mathematical pattern and stored in a computer. In iris recognition, the Biometrics is more reliable than traditional identifiers such as driver's licenses and identification or swipe cards because it relies on individually unique characteristics. And because it is tied to a computer, biometrics is fast and provides a record that other methods usually do not.

camera takes a picture of a person's eyes. The image is fed into a computer, which compares that image with ones already in its files until it finds—or fails to find—a match.

Seeking Security in New Jersey

New Egypt is a small town in rural southern New Jersey about 45 miles east of Philadelphia. The school system has about 1.700 students in three schools—an elementary, middle, and a new high school. New Egypt school officials were unaware of biometrics in 2002 when they realized their schools needed a new security system. At the time, the schools used a swipe-card system that was aging and did not always work. Plus, there weren't enough cards for everyone who needed one. School officials knew they had to improve not only the perception, but also the reality of school safety. They sought to develop a security system that would allay concerns and control access into the school buildings better than the swipe cards. They also wanted to use an innovative technology that could serve as a model for others.

After considering alternative biometric technologies, New Egypt officials chose iris recognition, one of the most reliable systems. Unfortunately for the school district, no complete iris scanning system existed that could be purchased and installed off the shelf. Instead, working with private vendors and NIJ, the school system developed its own iris recognition system. New Egypt was able to buy 11 existing cameras, placing 6 inside and 5 outside the elementary school's doors. Vendors had to write new software packages that would allow the cameras to send data images of scanned irises to a computer, tell the computer to search for a match, and then allow the computer to unlock the school doors once an individual's identification was confirmed.

As the iris recognition system was being developed, school officials kept parents informed of the plans and encouraged them to participate in the voluntary program. All told, nearly all of the schools' teachers and staff members and more than 700 elementary school parents had their eyes scanned into the system. The middle and high schools were not included in the test because far fewer of their students were taken out of class by parents or other family members during the school day.

A Passing Grade

cognition seemed parents, and staff e school. For the most part, iris recognition worked. Of the more than 9,400 times someone attempted to enter the school using the iris scanners, there were no known false positives or other misidentifications. Indeed, the system provided an accurate identification and unlocked the door 78 percent of the time. Of the failed attempts, 6 percent resulted from people using the scanners who were not enrolled and thus whose iris scans were not in the computer. Another 16 percent were due to problems with outdoor lighting or someone not lining up his or her eyes properly for the camera to read accurately.

> Most importantly, the iris recognition program seemed to make parents, teachers, and staff members feel safer in the school. When questioned as part of an outside evaluation of the program by 21st Century Solutions, parents who responded to the survey said at first they perceived little or no change in the efficiency of the sign-in process, the security problems within the school, or in the overall safety of the school neighborhood. Later, as people got used

to the scanners, most parents said they believed the T-PASS system provided greater security than the previous swipe-card one and was easier to use than ringing a buzzer and waiting for someone to open the doors. They also reported being able to enter and leave the school much more quickly when picking up their children during school hours than were parents who continued to sign in and out manually.

Similarly, teachers and staff members at the elementary school told program evaluators that they perceived school security as significantly increased. They felt that problems such as outside people getting into the schools easily and staff members leaving doors propped open had declined. The elementary school secretaries, in particular, reported fewer parents walking around the school looking for their children.

Still Some Problems

Some problems with the new iris scanners and security system arose, as one would expect of any new technology. For example, during the first few days the cameras often froze up and would not work. Some felt that the signs telling people how to use the scanners (or the traditional buzzers for people who had not yet had their eyes scanned) were confusing. And as noted above, some people could not seem to line up their eyes properly so the cameras could accurately scan them.

The latter problem was particularly acute among older staff members and among people who have a dominant eye. It was partly overcome by advising people to try a second or even a third time. In some cases, school officials spent extra time showing people how to position their head so the camera could accurately read their iris. Schools in Freehold Borough, the next New Jersey district to test the iris recognition system under an 18-month, \$350,000 NIJ grant, will use newer cameras that have two lenses rather than one. That will provide a more accurate reading even when people still cannot align their eyes properly.

The iris recognition program seemed to make parents, teachers, and staff members feel safer in the school.

A more serious problem was related to the use of outdoor cameras. Those cameras often failed to correctly identify people whose irises had been scanned, especially when they were in direct or bright sunlight. There were even problems accurately reading irises on gray, cloudy days. Most of the 16 percent failures noted above were due to sunlight affecting how the cameras could read the irises. In some cases, these problems could be overcome by placing a hood over the outside cameras to shield them from the sun.

Other problems had less to do with the technology or computers than with personal behavior. Many well-meaning students, teachers, and parents-once their irises had been scanned and the computer had unlocked the door for them-held the door open for another person entering the building behind them. Though the intent was good, the practice let others enter the school without having their irises scanned. Known as "tailgating," the problem declined when school officials reminded teachers, staff, parents, and students not to hold the door open even if they knew the second entrant. Additionally, both the New Egypt and Freehold schools are installing laser beams emanating from the ceiling that will detect a second, unscanned individual attempting to enter the building behind someone else and sound a buzzer in the school office.

A similar problem involved teachers, staff members, and others who went outside the school on their lunch break or between classes to eat, smoke, or talk to their colleagues. Often, these individuals propped open a door behind them so they could get back into the building easily without going through the iris scanners again. School officials even found a brick placed by one door, used to prop it open. Again, the problem declined when officials reminded school employees and parents of the need to keep the doors closed and locked for security reasons.

Finally, before the iris recognition system was installed at the New Egypt elementary school, some parents expressed concern about privacy issues and the sharing of data among computer systems. To safeguard the personal information of parents and students using the system, the school recorded only the user's name and driver's license or other personal identification number. School officials promised users that their names and personal information would not be shared with any other data systems. Teachers and staff had their Social Security numbers and home addresses entered into the system, but that data represented information the school already had.

In the end, NIJ and New Egypt school officials concluded that the iris recognition experiment showed promise. As one school official put it: "The project helped build community pride. We were the first to do this. In 20 years, you'll see biometrics in schools all over. All you have to do is look into a camera."

The evaluators note, however, that there is little research on the overall effects of access control technologies on school safety. Most of the so-called "normal crimes"-minor thefts and assaults-that characterize daily life in American schools are committed by people who are supposed to be there. Because access control technologies such as the iris scanner are really targeted toward keeping out those who are not supposed to be in the building, the technologies' impact on this type of crime is likely to be limited. And because outsiders constitute such a small minority of the people who commit crime in schools, the impact of these technologies might even be difficult to detect. So biometrics technologies such as the iris scanner should be considered as only one possible element in a school's overall safety plan.

NCJ 214114

For More Information

 Uchida, C., E. Maguire, S. Solomon, and M. Gantley, Safe Kids, Safe Schools: Evaluating the Use of Iris Recognition Technology in New Egypt, New Jersey, final report submitted to the National Institute of Justice, Washington, DC: 21st Century Solutions, Inc., August 2004 (NCJ 208127), available at www.ncjrs.org/ pdffiles1/nij/grants/208127.pdf.



Maximize Your Evaluation Dollars

by Edwin Zedlewski with Mary B. Murphy

About the Authors

Edwin Zedlewski is the Acting Deputy Assistant Director for Research and Evaluation at NIJ. Mary B. Murphy is the Managing Editor of the *NIJ Journal*.

> ou are a State program administrator and want to know the impact your programs have. One statewide program provides mentors to both teens and their parents. Should you try to discover whether the mentored teens are less prone to delinquency? If you find that they are, should you dig deeper and determine if it is because of the teen mentor or the parent mentor?

You are a county manager who funds a local program that makes housing and transitional services available to offenders returning to their communities. Could an evaluation decipher which aspects of the program are the most influential in determining whether clients recidivate?

You manage a Federal program supported in part by funds from an Attorney General's initiative to make troubled families more functional. How can you increase the program's prospects for success?

One of the most important aspects of managing a criminal justice program is ensuring that the program is meeting its objectives. An evaluation is the best way to accomplish that.

But evaluations can be expensive, particularly evaluations to identify the precise impact a program is having. A rigorous, scientific impact evaluation typically costs NIJ between \$500,000 and \$1.5 million. A poor choice about which programs are suitable for evaluation is more than just a waste of time—it's a waste of millions of dollars.

The NIJ Approach: An Evaluability Assessment

NIJ has developed a way to identify programs that are likely to yield evaluations that maximize the agency's return on its

investments. By adopting NIJ's approach, program administrators at all levels of government may save considerable time and money.¹

The first step is to assess a program's "evaluability"—that is, to gauge which programs can sustain a rigorous outcome evaluation. The evaluability assessment takes 1 to 5 days and is guided by some common sense questions:

- Are program components stable or still evolving?
- Can we trace logical and plausible connections between a program's activities and its intended outcomes?
- Are there enough cases or observations to permit statistically robust conclusions?
- Can we isolate the program's effects from other related forces operating in the community?

Many programs can be summarily rejected after answering these initial questions. For example, a program that has few participants would be unsuitable for a rigorous, scientific evaluation. Alternatively, one that would require 10 to 20 years of followup is not a practical candidate for a low-cost, 2-year evaluation.

Take a Closer Look

Next, NIJ reads the complete files of potential programs. Programs that are funded through a grant, for example, will have a grant application that explains the program's goals and activities, developmental history, quality of the data systems, and numbers of clients served. Typically, the initial screening involved in this step reduces the list of candidates to 20 to 25 percent of the original pool.

If additional insight is needed, evaluators can conduct telephone interviews with the program's management, review progress reports and other grant materials, and gather other information to answer NIJ has developed a way to identify programs that are likely to yield evaluations that maximize the agency's return on its investments. By adopting NIJ's approach, program administrators at all levels of government may save considerable time and money.

outstanding questions about the programs. They should ask the following questions:

- What do we already know about programs like these from the research literature?
- What could an evaluation of this program add?
- Which audiences would benefit from an evaluation and what could they do with the findings?
- Are the program managers interested in being evaluated?
- Is the program director already planning an evaluation? If so, evaluators should further inquire:
 - What data systems exist that would facilitate an evaluation?
 - What key data elements are contained in these systems?
 - Are there data to estimate unit costs of services or activities?
 - Are there data about possible comparison samples?
 - How useful are the data systems to an impact evaluation?

Program managers must be able to explain how the program's primary activities contribute to its eventual goals and identify other local programs serving similar populations that could be used for outcome comparison.

Evaluability assessments not only guide decisions about which programs are good candidates for an outcome evaluation, they also help evaluators develop the research design and estimate the cost.

Conduct a Site Visit

If the program seems promising after a rigorous screening, a site visit may be in order. Site visits usually take an entire day and spark rich interactions that reveal operational strengths and flaws that might not otherwise be visible.

During a site visit, evaluators should determine:

- If the program is being implemented as described in the application.
- What components of the program would be the most sensible to evaluate.
- What outcomes could be assessed and by what measures.

Next, evaluators should speak with the following individuals:

Key program staff.

Do staff members tell consistent stories about the program? Are their backgrounds appropriate for the program's activities?

Program partners.

What services do partners provide or receive? How integral are they to the success of the program? What do partners see as the program's strengths and weaknesses?

Program director.

Does the director understand the demands that an evaluation will place on staff? Will the director make the changes necessary to support the evaluation? Assess the Target Population. Evaluators should determine a number of factors about the target population—its size, its characteristics, and the way in which program staff identify it. Is entry into the program voluntary? Who will be excluded from the program? Evaluators also must learn if participants' characteristics have changed over time, and whether there are shortcomings or gaps in how the program delivers the intervention.

Evaluators then must decide whether to interview members of the target population or program participants. If interviews are conducted, participants should be asked what they think the program does and how they would assess the services received. This information is invaluable in assessing the success of the program, identifying problems in its implementation, and improving the delivery of services in the future.

Examine the Data. Evaluators should then examine data systems to identify what kind of data are available; whether it is complete; whether routine reports are produced; and what specific input, process, and outcome measures the data support. Do the data systems follow participants over time, and if so, do the records allow evaluators to identify services delivered to each individual?

Evaluators need data systems that are organized, complete, and current—or else be prepared to spend considerable time and resources collecting data and implementing quality control measures.

Select Evaluation Design. Using the information gathered during the screening and site visit, evaluators must then determine the best evaluation design. The answers to a few key questions will aid in that decision:

- Are there enough participants so evaluators can make random assignments to test and control groups?
- If there are not enough participants, can the evaluator find a highly comparable group (with similar demographics, risk factors, and so forth) that does not receive services?

- How large would program and comparison samples be after the intended period of observation?
- What services would a control or comparison sample receive?

Finalizing the Assessment Recommendation

At the conclusion of the assessment process, evaluators write a report that recommends whether the program should be evaluated. The reports typically contain all the information collected, including sample data forms and program brochures, and discuss the ramifications of various design options.

Evaluability assessments not only guide decisions about which programs are good candidates for an outcome evaluation, they also help evaluators develop the research design and estimate the cost. Assessments also initiate and foster relationships that will prove helpful when evaluations reach rocky points and negotiations become necessary.

This process has worked well for NIJ. State and local agencies can achieve a similar level of success and minimize evaluation risks by following NIJ's approach to evaluability assessments.

NCJ 214115

Note

1. NIJ doesn't limit its assessments to those programs most likely to succeed. Sister agencies in the Office of Justice Programs occasionally develop programs in high priority areas where problems are just emerging. These programs need to evolve and stabilize before they are ready for a formal evaluation. For these types of programs, evaluability assessments have helped NIJ pinpoint which areas require development and commission a formative evaluation—one that provides constructive feedback to both the program and the program office and that suggests improvements.



Advancing Justice Through DNA Technology

Online Training

A comprehensive online course on the use of forensic DNA in judicial proceedings is now available at www.dna.gov/training/otc. Broken down into 15 modules, this tutorial provides an introduction to DNA analysis and the legal issues surrounding DNA evidence. While the course was originally designed for prosecutors, defense attorneys, and judges, the information covered will also interest the public. Topics include:

- The biology of DNA, including statistics and population genetics.
- DNA laboratories, quality assurance in testing, and understanding a laboratory report.
- Forensic databases.
- Victim issues.
- The presentation of DNA evidence at trial.
- Post-conviction DNA cases.





Digital Evidence: How Law Enforcement Can Level the Playing Field With Criminals

by Nancy Ritter

About the Author

Nancy Ritter is a writer/editor at the National Institute of Justice.

he need for State and local police departments to leap ahead in the war on cyber-crime and develop procedures for identifying and processing electronic evidence is urgent. Yet, progress continues to be slow.

"At the rate we're going now, law enforcement is going to fall so far behind the electronic technology curve that, in a couple of years, we will *never* catch up," says Bob O'Leary, a former New Jersey detective, who heads up the Electronic Crimes Partnership Initiative (ECPI).

Funded by the National Institute of Justice, ECPI is a multidisciplinary team of professionals committed to enhancing law enforcement officers' ability to solve computer crimes. ECPI draws on the skills of a coalition of experts from law enforcement, academia, the government, and the private sector. The experts at ECPI teach police officers to solve computer crimes (such as using the Internet for child pornography) and to develop digital evidence (from computers or cell phones, for example) in crimes like rape and murder.¹ By educating law enforcement professionals on the myriad ways computers can facilitate criminal acts, the group seeks to help officers conduct more sophisticated investigations that will build stronger cases and lead to more convictions.

The Importance of Cyber Education

Each day, State and local law enforcement officers must identify, gather, and analyze both physical and electronic evidence in a wide range of cases. Most police officers are skilled at recognizing physical evidence in such cases, but many have never been trained to recognize the existence or importance of electronic evidence in solving a crime or building a winning case.

And they aren't the only ones in the dark. A recent NIJ needs-assessment study found that many police chiefs, senior managers, and those who make funding and resource allocation decisions do not possess the level of expertise or tools needed to investigate and prepare cases for successful prosecution. Guy Meader, an electronic crime technology analyst at NIJ and former detective in Montgomery County, Maryland, adds, "Of the police chiefs and managers who *are* willing to support an investigative capability for electronic crime, they often do so at the expense of other units or assign dual investigation responsibilities to personnel."

To help law enforcement professionals use electronic tools in fighting crime, ECPI is developing a 4-year, bachelor's degree curriculum that will award graduates a degree in Electronic Crime Prevention and Investigation. The degree will combine inthe-field investigative skills—the ability to see the big picture, whether through understanding a suspect's *modus operandi* or approaching a physical location—with digital know-how.

ECPI also is working with the nonprofit volunteer group International Association of Computer Investigative Specialists (IACIS) on a "Bag-'n-Tag" course to teach officers how to seize and process digital evidence, which is often more fragile and fleeting than other physical evidence at a crime scene. ECPI and IACIS will hold classes in police departments, universities, and prosecutor's offices around the country.

O'Leary emphasizes the importance of the Bag-'n-Tag course. "It's crucial that you get everything from a crime scene the first time," he says, "because you often don't get to go back [without a new warrant]." By then, the scene may have been compromised, and critical evidence removed or destroyed.

Eliminating Impediments to Prosecution

One of the greatest challenges in electronic crimes for law enforcement is the absence of geographic boundaries. Ed Kelly is an Assistant United States Attorney for the By educating law enforcement professionals on the myriad ways computers can facilitate criminal acts, the group seeks to help officers conduct more sophisticated investigations that will build stronger cases and lead to more convictions.

Southern District of Iowa and is currently on detail to NIJ as a senior advisor on electronic crime. Kelly explains that while the Internet has eliminated boundaries for criminals, State and local officials' investigative authorities still are bound by narrowly defined jurisdictional areas. These boundary restrictions and the resulting conflict of authority often mean that officers must apply for warrants in multiple jurisdictions. This extra footwork can translate into a loss of valuable time and, ultimately, evidence.

ECPI is working on a way to encourage reciprocity (sometimes called "full faith and credit") between States when outof-State search warrants, subpoenas, and court orders are served. Kelly, who is also a former assistant director for cyber-crime training of Federal prosecutors at the U.S. Department of Justice's National Advocacy Center, said ECPI is investigating how reciprocity can best be pursued.

Another impediment to prosecuting cybercrime cases is the time it takes for Internet service providers (ISPs) to respond to subpoenas. Currently, it often takes several weeks for an ISP to produce subpoenaed records. ECPI is working on a way to facilitate responses. Using secure servers in strategic locations around the country, ISPs could transfer records much more quickly to a regional server to which only designated law enforcement personnel would have access. ISPs, which are often served with hundreds of subpoenas a day, have voiced support for the idea, because it would save them significant reproduction time and

First on the agenda is an assessment of the tools that law enforcement needs to catch cyber-criminals and stay ahead of the electronic technology curve. Criminal justice professionals must look beyond the immediate horizon, says O'Leary, and a new needs assessment will help them do that.

> costs. And, from a law enforcement perspective, a faster response increases the potential for more successful investigations and prosecutions.

The Need for Standards

Whenever a new field of investigation burgeons, a need to establish standards soon surfaces. Thus, ECPI is working to establish standards for the collection and analysis of digital computer evidence and to create uniform standards for the certification of examiners. Mike McCartney is a senior investigator with the Criminal Investigations Division of the New York State Attorney General's Office and member of ECPI's standards and certification working group. McCartney notes that although some standards exist for digital evidence forensics, the certification of examiners varies widely. And there are no standards or certifications for high-tech crime investigators.

McCartney's group is exploring standards and certifications that will apply to personnel, education and training programs, tools, and forensics labs. The group is also establishing guidelines for conducting investigations, handling and preserving evidence, and prosecuting cases.

Going Forward

ECPI also has plans to update NIJ's publications on e-crime and digital evidence. First on the agenda is an assessment of the tools that law enforcement needs to catch cyber-criminals and stay ahead of the electronic technology curve. Criminal justice professionals must look beyond the immediate horizon, says O'Leary, and a new needs assessment will help them do that.

NCJ 214116

Note

 ECPI was created after an NIJ needsassessment study (*Electronic Crime Needs Assessment for State and Local Law Enforcement*, NCJ 186276) concluded that "any potential for growth in electronic crime raises serious concerns about the capability of law enforcement resources to keep pace."

DIGITAL EVIDENCE IN HIGH-PROFILE CASES

Martin Novak, program manager of NIJ's e-crime portfolio, illustrates how digital evidence know-how helped solve several recent highprofile crimes:

- BTK serial murderer Dennis Rader terrorized Wichita, Kansas, for 30 years until evidence on a computer disk led police to the former church council president and Cub Scout leader.
- Scott Peterson's computer contained a map of the island where his wife's body was found and revealed that he had shopped online for a boat, studied water currents, and bought a gift for his mistress.
- David Leslie Fuller's computers showed that he had stalked three other teenage girls before he abducted, raped, and murdered 13-year-old Kacie Woody, whom he met in an online chat room.

NIJ and Harvard University Webcast Addresses Prisoner Reentry

Inmate reentry, the transition from life in a prison or jail to life in the community, has profound implications for public spending and public safety.

In November 2005, the NIJ/Harvard University Webcast series explored the challenges prisoners face reintegrating into society.

"Prisoner Reentry: Facing the Challenges of Returning Home" tapped the knowledge and experience of key leaders in reentry research and program development, highlighted housing programs designed to assist returning prisoners, and discussed the resulting policy changes for lawmakers.

Speakers included:

- Jeremy Travis, president of the John Jay College of Criminal Justice, author of But They Came Back: Facing the Challenges of Prisoner Reentry, and former NIJ Director.
- Terry Donahue, associate director of the Community Capacity Development Office, U.S. Department of Justice.
- Georgia Lerner, associate executive director for program operations at the Women's Prison Association.

Produced by Harvard University's Ash Institute for Democratic Governance and Innovation, NIJ, and OJP, the NIJ/Harvard Webcast series focuses on innovations in public safety. Multimedia presentations of all sessions and announcements of future programs can be found on the Ash Institute's Government Innovators Network Web site at www.innovations.harvard.edu.



Methamphetamine Abuse: Challenges for Law Enforcement and Communities

by Dana E. Hunt

About the Authors

Dana E. Hunt is a Principal Scientist at Abt Associates Inc. Sarah Kuck, a Senior Analyst at Abt Associates Inc., contributed to this article.

ifty-eight percent of county law enforcement agencies surveyed by the National Association of Counties in 2005 listed methamphetamine as the number one drug problem in their area. States as diverse as Arkansas, Indiana, Vermont, and Wyoming reported increases of more than 90 percent in methamphetamine arrests in the prior year. Cheap, easy to manufacture, and long lasting, methamphetamine has become more popular than cocaine in some U.S. cities. And the problem is no longer confined to discrete regions of the country.

Why is methamphetamine abuse such a growing problem, and what should police and communities do to combat this threat? The final report of a study funded by the National Institute of Justice provides findings that State and local law enforcement and public safety officials need to know to answer these questions.¹

Statistics Belie the Extent of the Problem

Methamphetamine is a completely synthetic drug. Refinements to inexpensive manufacturing methods in the 1980's and 1990's led to abuse in epidemic proportions in areas of the West and Midwest. By the millennium, the drug had taken hold in the South and Midwest. While methamphetamine use has been consistently high in States such as California, Hawaii, Idaho, and Nevada,² self-reported use among adults nationwide has risen from just under 2 percent in 1994 to around 5 percent in 2004.³ Treatment admissions data reflect that the national rate of treatment for methamphetamine abuse rose from 1 percent in 1992 to more than 6 percent in 2003.4

But national data are misleading. While these figures reflect increases at low levels on a national scale, regional data gathered from clients entering drug treatment provide a far more serious picture of the problem and

chronicle both its remarkable increase and its geographic movement.⁵ In 1992, no State reported that 10 percent or more of all of its treatment admissions were for methamphetamine. By 2003, however, 35 percent of States reported more than 10 percent of all admissions were for methamphetamine, and 8 States reported an admissions figure of more than 20 percent.⁶ While the highest rates were found in Hawaii (45 percent), Idaho (42 percent), and California (31 percent), Midwestern States such as Iowa, Minnesota, Montana, Nebraska, and North Dakota also saw large increases. Southern States such as Arkansas increased their numbers tenfold or more.⁷

Regional differences in data on emergency room (ER) visits for methamphetaminerelated problems are similarly dramatic.⁸ While rates in some cities with high numbers of ER visits for problems related to methamphetamine use have remained unchanged or even declined somewhat, rates in other areas have experienced enormous upswings since 1995. These include Minneapolis (up 243 percent), New Orleans (up 194 percent), St. Louis (up 97 percent), and Atlanta (up 67 percent).⁹ These local trends were mirrored in NIJ's Arrestee Drug Abuse Monitoring (ADAM) system data. In 11 ADAM sites studied in 2003, 25 percent of arrestees tested positive for methamphetamine in their systems; by contrast, only 1 ADAM site had a proportion that high in 1996.¹⁰

A Specialized Approach

Everything about methamphetamine from its composition to its manufacturing and distribution systems and the physical effect it has on its users—is unique. And these distinctions require that law enforcement officers adopt specialized approaches to criminal investigations and arrests.

Unlike imported drugs such as heroin or cocaine, methamphetamine is easy to produce domestically. It is synthesized from precursor chemicals using relatively easy production methods that are commonly available on the Internet or in underground publications; anyone with high school chemistry experience can "cook" *Cheap, easy to manufacture, and long lasting, methamphetamine has become more popular than cocaine in some U.S. cities.*

methamphetamine. Many of the base chemicals are household or farm products that are not feasible to regulate. However, other elements (ephedrine and pseudoephedrine products, and anhydrous ammonia) have come under serious scrutiny, and Federal and State legislation now monitors their sale and limits their availability.¹¹ Unfortunately, as restrictions effectively close "Mom-and-Pop" operations—also known as small toxic labs or STLs—the demand for methamphetamine remains. Law enforcement in many areas reports increased evidence of organized drug traffickers, largely from Mexico, covering the established demand.

Although the number of small "Mom-and-Pop" labs is far greater than the number of superlabs (labs capable of making 10 or more pounds of product at a time), the Drug Enforcement Administration (DEA) states that the bulk of methamphetamine on the U.S. market comes from superlabs concentrated in the Central Valley and southern areas of California or in Mexico. Data show that the presence of superlabs in the United States is expanding. Historically, precursor chemicals were smuggled to superlabs in the Southwest and California, but the current distribution is more geographically dispersed throughout the country. DEA's Clandestine Laboratory Seizure System reports that the number of superlabs seized in the western regions has actually declined by half between 1999 and 2004, but has doubled in the South. And while seizures of methamphetamine powder have declined in some areas, officials report an increase in seizures of the higher potency crystalline form not generally made by local "cooks."

Meth Labs Pose Dangers for Law Enforcement and Communities

The way that methamphetamine is manufactured and distributed hinders law enforcement officers' ability to locate and shut

Everything about methamphetamine from its composition to its manufacturing and distribution systems and the physical effect it has on its users—is unique. And these distinctions require that law enforcement officers adopt specialized approaches to criminal investigations and arrests.

> down smaller labs. First, detection of these laboratories is difficult due to their clandestine placement in rural settings where law enforcement resources are limited. Second, criminal investigations are also hindered by the fact that—unlike sales of crack and heroin-most methamphetamine sales take place indoors, out of the view of police surveillance. Also, much of the methamphetamine produced in "Mom-and-Pop" labs is consumed by the manufacturers or sold to a very small group of friends or acquaintances. This close-knit distribution system impedes law enforcement officers' ability to use traditional investigative methods to infiltrate a distribution group and identify offenders, target laboratories, and take down operations.

> Methamphetamine laboratories also pose a serious danger to law enforcement officers. The use of toxic and combustible chemicals makes executing search warrants at meth laboratories a dangerous undertaking. In fact, reports of injuries to responding law enforcement officers have almost doubled from 2002 to 2003.12 Whether the laboratory is raided by investigators or encountered by accident during the course of an operation, first responders and police agencies require specialized training and equipment. Hermetically sealed hazmat suits, licensed contractors, and specialized training in how to safely process the scene are expensive resources that are in limited supply in local law enforcement agencies.

Methamphetamine production and use also negatively impact the quality of life in areas where it has taken hold. For example, child protection service agencies across affected areas are inundated with cases involving the removal of children endangered by chemicals and toxic fumes. Child neglect cases also abound in areas where methamphetamine use and production exists.

Methamphetamine laboratories also contaminate surrounding property. It is estimated that 1 pound of methamphetamine produced in a clandestine lab yields 5 to 6 pounds of hazardous waste.¹³ The resultant environmental damage to property, water supplies, farmland, and vegetation where labs have operated costs local jurisdictions thousands of dollars in clean up and makes some areas unusable for extended periods of time. Damage to some areas is extensive. For example, U.S. Forest Service officers have encountered tree "kills" in areas surrounding STLs, and ranchers in Arizona have reported suspicious cattle deaths in areas downstream from labs.¹⁴

These findings demonstrate that methamphetamine is not just an issue for law enforcement to contend with—it's an entire community's problem.

The Methamphetamine Abuser: Not Your Ordinary Addict

Available data on typical methamphetamine users reveal that most are white, are in their 20's or 30's, have a high school education or better, and are employed full- or part-time. Methamphetamine is used by housewives, students, club-goers, truckers, and a growing number of others. Almost as many women as men use methamphetamine (55 percent male, 45 percent female.)

But a methamphetamine user is not the typical drug user. That is because methamphetamine has acute toxic effects that produce long-term problems for the user and those around him/her. It is a powerful central nervous system stimulant that

promotes the release of neurotransmitters that control the brain's messaging systems for reward and pleasure, sleep, appetite, and mood. However ingested (injected, taken orally, or snorted), methamphetamine produces extended highs and potentially agitated or overenergized states.

Chronic use of methamphetamine causes long-term alterations to users' brain chemistry and structure that result in impaired memory, mood alterations, impaired motor coordination, and psychiatric problems, even long after terminating use. The short-term management of the agitated user at arrest and the long-term health problems that jails and lock-ups must deal with make methamphetamine users a serious logistical and financial burden, particularly in areas with limited manpower or resources.

Meth Matters

Methamphetamine—once only a regional problem of the West and Northwest has hit Midwestern and Southern States hard and is moving east. Methamphetamine is cheap and easy to manufacture, and profit margins are high. Its powerful stimulant effect has made it more popular than cocaine in many areas. It is a drug that appears to move easily into new areas not typically associated with drug trafficking, where smaller labs serve local groups of users. As a demand or market is established, however, more organized manufacturers and distributors are attracted.

Methamphetamine presents major challenges and resource demands for State and local public safety and law enforcement. The implementation of community resource coordination, joint agency initiatives, and development of new skills and partnerships are essential steps to take on the challenges presented by methamphetamine abuse.

NCJ 214117

For More Information

 Pennell, S., J. Ellet, C. Rienick, and J. Grimes, *Meth Matters: Report on Methamphetamine Users in Five Western Cities*, Research Report, Washington, DC: U.S. Department of Justice, National Institute of Justice, April 1999 (NCJ 176331), available at www.ncjrs.gov/ pdffiles1/176331.pdf.

Notes

- Hunt, D., S. Kuck, and L. Truitt, *Methamphetamine Use: Lessons Learned*, final report to the National Institute of Justice, February 2006 (NCJ 209730), available at www.ncjrs. gov/pdffiles1/nij/grants/209730.pdf.
- 2. Ibid., 13 (Table 1.4).
- 3. Ibid., 7 (Figure 1.1).
- 4. Ibid., 12 (Figure 1.3).
- Ibid., 11. The Treatment Episode Data Set (TEDS) represents information gathered from clients at admissions to each episode of treatment in programs across the country.
- 6. Ibid., 13 (Table 1.4).
- 7. Ibid.
- Ibid., 14 (Table 1.5). The Drug Abuse Warning Network (DAWN) is a system of data abstraction from the records of a nationally representative set of hospital emergency departments. DAWN provides area level and national estimates of the number of emergency department episodes that involve various drugs and the reason for the visit.
- 9. Ibid.
- 10. lbid., at 15, 16 (Figure 1.4).
- 11. Tennessee, for example, found legislation placing over-the-counter cold medications containing ephedrine/pseudoephedrine behind the pharmacy counter reduced the number of "Mom-and-Pop" or small local labs seized from more than 1,500 in 2004 to 955 in 2005, with the most dramatic reductions seen in rural counties. (Data presented by Thomas Scollon, Tennessee Office of Criminal Justice Programs, Nashville, Tennessee, at the Evaluation of Task Forces Cluster Meeting held at the National Institute of Justice in Washington, DC, in January 2006.)
- 12. Hunt et al., "Methamphetamine Use: Lessons Learned," 26.
- 13. Ibid.
- 14. Ibid.



Has Rape Reporting Increased Over Time?

About the Author

Lauren R. Taylor is a freelance writer.

uring the past three decades, women have become more likely to report rapes and attempted rapes—particularly those involving known assailants—to police. Reporting by others, such as friends and family members, has also risen.

Past studies have shown increases in reporting, but they did not consider changes in the types of incidents occurring or being reported. "Reporting trends without the details—such as crime completion, presence of a weapon, or victim-offender relationship can be misleading," researcher Eric Baumer points out. "Changes in willingness to report can be confused with changes in the nature of the crimes themselves." So Baumer aimed for a more comprehensive study that considered such details.

He used data from the National Crime Survey (NCS) (1973–1991)¹ and National Crime Victimization Survey (NCVS) (1992–2000)²

to find out how reporting has changed over time, who does the reporting, and the effect of the victim-offender relationship on the chance a rape will be reported. Baumer's research included all incidents involving a female victim and one or more male offenders (1,609 from 1973–1991, and 636 from 1992–2000).

Subjects interviewed in the National Crime Survey were not asked directly about rape. However, when the survey was redesigned in 1992 and renamed the National Crime Victimization Survey, interviewers began asking a series of questions about "unwanted sexual activity." The number of sexual victimizations disclosed to interviewers in the second survey shot up, and fewer of them had been reported to police. Because of the survey redesign in 1992, data from the two periods cannot be compared.

Baumer also compared rape reporting with the reporting of other kinds of assaults to see whether broader social changes—such

as declining social supports in the wake of violent crime—may have been associated with the changes. He found no significant increase in the likelihood of police notification of other types of assaults, so the increase was particular to rape.

The Rapist You Know

In the 1970's and 1980's, most of the increase in reporting was not from victims, but from third parties (friends, family members, or legal advocates). Among victims, the biggest increase in reporting was in cases where women had been attacked

by people they knew. Historically, such cases had been much less likely to be reported. As a result of this large increase, the gap between the reporting of knownassailant cases and stranger cases narrowed. During the 1990's, reporting of rapes committed by known assailants and strangers increased both among third parties and victims. By this time, sexual assault was equally likely to be reported to the police, whether or not the victim knew the offender, though third parties were still less likely to report if the assailant was known to the victim.

PREDICTED PROBABILITIES OF POLICE NOTIFICATION FOR FEMALE VICTIMS OF RAPE, 1973–2000

In the 1970's and 1980's, the likelihood that police would be notified of a rape if the victim knew the assailant increased faster than the likelihood of reporting if the assailant was a stranger. As a result, by the early 1990's, the difference in the likelihood of reporting stranger and nonstranger incidents had become quite small. That trend continued throughout the 1990's, although an expansion of the survey in 1992 to include data on "unwanted sexual activity" revealed that fewer of those incidents were reported to the police. These statistics are illustrated in the following chart.



Social and political movements along with changes in the law encouraged women to inform police about sex crimes.

A Changing World

During the 1970's, 1980's, and 1990's, transformations were taking place in the way Americans defined and responded to rape. Social and political movements—along with changes in the law—encouraged women to inform police about sex crimes. Academics, victim service providers, law enforcement officers, and others continue to debate how these shifts affected perceptions of women, rape, and sexual behavior. But most important, queried Baumer in his study, "Did these changes alter behavior?"

Baumer didn't study the effects of changing attitudes on reporting, but he believes his research can be used to assess them indirectly. He suggests that the increases he found were consistent with changes in law and culture that removed many of the institutional and social barriers to reporting.

Reporting increases were greatest among women raped by acquaintances especially well-known acquaintances, spouses, or ex-spouses. This makes sense, Baumer believes, given the focus of legal and social reforms on broadening the definition of rape and reducing obstacles to prosecution in such cases.

A Hidden Crime?

Although legal, social, and political reforms appear to have improved the chances that a rape or attempted rape will be reported to police, most victims still do not report. Between 1992 and 2000, an average of 31 percent of attempted and completed rapes were reported.³ That rate increased over the decade, but the fact remains that less than half of such crimes are reported to police.

Baumer suggests that work be done to identify the policies or practices that encourage reporting and to apply those practices elsewhere. Such a strategy might, in turn, increase the chance of arrest and prosecution and, ultimately, the deterrent effect of the criminal justice system.

NCJ 214118

For More Information

 Baumer, E., Temporal Variation in the Likelihood of Police Notification by Victims of Rapes, 1973-2000, final report submitted to the National Institute of Justice, Washington, DC: University of Missouri-St. Louis, April 2004 (NCJ 207497), available at www.ncjrs. gov/pdffiles1/nij/grants/207497.pdf.

Notes

- National Crime Surveys: National Sample of Rape Victims, 1973–1982, Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, 1985 (NCJ 104624); National Crime Surveys: National Sample, 1979–1987, Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, 1989 (NCJ 130249); National Crime Surveys: National Sample, 1986–1992, Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, 1994 (NCJ 175690).
- National Crime Victimization Survey, 1992– 2000, Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, 2001, available at webapp.icpsr.umich.edu/cocoon/ NACJD-STUDY/03140.xml.
- Reporting Crime to the Police, 1992– 2000, Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, 2003 (NCJ 195710):1, available at www. ojp.usdoj.gov/bjs/pub/pdf/rcp00.pdf.

The National Institute of Justice is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development, and evaluation to enhance the administration of justice and public safety.

> The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Photo Sources: PictureQuest and PunchStock

U.S. Department of Justice

Office of Justice Programs *National Institute of Justice*

Washington, DC 20531 Official Business Penalty for Private Use \$300

NIJ