National Institute of Justice (NIJ): Improving the Effectiveness of Law Enforcement via Homeland Security Technology Improvements

Dr. John S. Morgan
National Institute of Justice
Assistant Director
for
Science & Technology

National Institute of Justice
810 Seventh St., NW
Washington, DC 20531

ABSTRACT

Law enforcement agencies play a key role in protecting the nation from and responding to terrorist attacks. Preventing terrorism and promoting the nation's security is the Department of Justice's number one strategic priority. This is reflected in its technology development efforts, as well as its operational focus. The National Institute of Justice (NIJ) is the national focal point for the research, development, test and evaluation of technology for law enforcement. In addition to its responsibilities in supporting day-to-day criminal justice needs in areas such as less lethal weapons and forensic science, NIJ also provides critical support for counter-terrorism capacity improvements in state and local law enforcement in several areas. The most important of these areas are bomb response, concealed weapons detection, communications and information technology, which together offer the greatest potential benefit with respect to improving the ability to law enforcement agencies to respond to all types of crime including terrorist acts. NIJ coordinates its activities with several other key federal partners, including the Department of Homeland Security's Science and Technology Directorate, the Technical Support Working Group, and the Department of Defense.

Key Words: National Institute of Justice, Technical Support Working Group, Department of Homeland Security Directorate of Science and Technology, weapons detection, through-the-wall surveillance, explosives detection and remediation, communications interoperability, information systems, law enforcement responder, state and local public safety agencies, SAFECOM, Information Led Policing.

1. NIJ's Role and Mission

NIJ is the research and technology development arm of the Department of Justice (DOJ). It is dedicated to researching crime control and justice issues, with an emphasis on the needs of the state and local criminal justice community. NIJ sits within the Office of Justice Programs (OJP). OJP comprises five bureaus and two program offices. The mission of OJP is to assist state and local criminal justice agencies prevent crime and improve their criminal justice systems. Other OJP components include the Bureau of Justice Assistance, the Office of Victims of Crime, The Office of Juvenile Justice and Delinquency Prevention, and the Bureau of Justice Statistics.

Sensors, and C3I Technologies for Homeland Security and Homeland Defense IV, edited by Edward M. Carapezza, Proceedings of SPIE Vol. 5778 (SPIE, Bellingham, WA, 2005) · 0277-786X/05/$15 · doi: 10.1117/12.606901

NIJ provides objective, independent evidence-based knowledge and tools to meet the challenges of crime and justice. Through its Office of Science & Technology (OS&T), NIJ serves as the national focal point for the research, development, test and evaluation of technology for law enforcement, corrections and forensic sciences. NIJ identifies the Criminal Justice Community's requirements for new technologies and develops the technologies to meet those requirements. NIJ also develops standards and testing programs to evaluate technologies that may be used by law enforcement agencies and works with other entities within DOJ and other federal agencies to establish a coordinated federal approach on issues related to law enforcement technology, including terrorism.

The Role of State and Local Law Enforcement in Counter-terrorism

NIJ's research program is primarily focused on the needs of state and local law enforcement, since the overwhelming majority of crime is adjudicated on the state and local level. State and local officials are the last line of defense in the prevention of terrorism. Many of the September 11, 2001 terrorists were listed in state and local law enforcement databases, and several were stopped by state and local law enforcement officers in the weeks leading up to September 11. In most cases, to this day, state and local law enforcement agencies lack the technology needed to fully analyze information about terrorism and other organized criminal activity. They also lack essential tools in bomb response, concealed weapons detection, and communications. In all of these areas, law enforcement agencies would use the needed technology on a daily basis to support routine operations and prevent violent crime.

NIJ's program is based on the assumption that terrorists must operate within the constraints presented to any organized criminal activity. Therefore, an effective counter-terrorism strategy for state and local law enforcement is to improve its ability to proactively deal with gangs, drug activity, identity theft, serial murder, and other organized crime. Since research indicates that terrorists routinely engage in these kinds of activities, a sophisticated law enforcement response to day-to-day crime will produce significant benefits in the war on terror. Obviously, this cannot be the only strategy for counter-terrorism, which also requires pre-emption overseas, infrastructure protection, detection of weapons of destruction, and effective response and recovery, among other priorities.

The Department of Homeland Security's Directorate of Science & Technology (DHS S&T) has the primary responsibility in the federal government for improving the nation's response to terrorist threats involving weapons of mass destruction (WMD's). Because terrorism is a criminal act, the more than 19,000 law enforcement agencies–most notably the state and local agencies, which will be among the first at the scene–play a key role in protecting the nation from and responding to terrorist attacks. Recognizing this and NIJ's central role in addressing the technology needs of the criminal justice community, Congress, in Public Law 107-296, directed NIJ to address law enforcement's technology needs to combat terrorism through its Office of Science & Technology (OS&T).

While DHS focuses on technologies to respond to WMD, NIJ focuses on technologies applicable across the spectrum of law enforcement needs. It addresses these technology needs by direct investment and by coordinating its efforts with those of other agencies. NIJ and DHS S&T executed a memorandum of understanding in June 2004, which provides a means for exchanging information regarding their respective research and technology efforts, for coordinating those efforts and for initiating joint efforts. NIJ participates on the Technical Support Working Group (TSWG), which is the locus of Federal counterterrorism research and development. NIJ also manages the DOJ Technology Policy Council, which is the forum for federal law enforcement technology development agencies.

Put simply, NIJ is involved in developing technology to combat terrorism because terrorism is a criminal act. By far the largest components of the responder community are the state and local public safety agencies. More than 90 percent of law enforcement agencies are state and local. State and local public safety responders will

be the first on the scene dealing with a terrorist incident. The most effective way to enhance the ability of law enforcement responders to deal with terrorist acts is to enhance their capacity to deal with critical incidents in general. A critical incident is defined as any major threat to lives and property. Such technologies must be developed with the understanding that the law enforcement responder does not operate in a vacuum, but rather acts as part of a coordinated, multi-disciplinary public safety response. The Institute's technology efforts are structured with an understanding of these realities. They focus on meeting the unmet technology needs of the law enforcement responder, and those needs that they have in common with other public safety agencies.

2. Command, Control, Communications and Intelligence (C3I) Challenges

Providing State and local public safety agencies effective communications and information systems remains a key technology challenge. Investment in C3I technology offers perhaps the greatest potential benefit with respect to improving the ability to the responder community to respond to terrorist attacks and other critical incidents. C3I provides the ability to predict and prevent, or that failing, to better plan and coordinate the response to a terrorist attack.

The highest priority technology need identified by practitioners in the *Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism*, which was conducted by the Institute in 1997, was for a national, intergovernmental information sharing system with current intelligence. Not far behind was the need for improved interagency communication and information sharing. These are technology challenges that NIJ and its technology partners–most notably perhaps with DHS S&T and SAFECOM—are aggressively addressing. (SAFECOM was established to serve as the umbrella program within the Federal Government, to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications.) Our efforts in this area are in large measure being focused through the Global Justice Information Sharing Initiative known as (GLOBAL).

GLOBAL

GLOBAL has a direct impact on the work of more than 1.2 million justice professionals. However, the importance of Global's mission–the efficient sharing of data among justice entities, which is at the heart of modern public safety and law enforcement–positions Global to impact citizens of the U.S., Canada, and beyond. Global is a "group of groups," representing more than thirty independent organizations spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Member organizations participate in Global out of shared responsibility and shared belief that, together, they can bring about positive change in inter organizational communication and data sharing.

Global aids its member organizations and the people they serve through a series of important initiatives. These include the facilitation of the Global working groups; development of technology standards such as the Global Justice XML Data Model; and the National Criminal Intelligence Sharing Plan.

The Global Justice XML Data Model

What began in March 2001 as a reconciliation of data definitions evolved into a broad two-year endeavor to develop an XML-based framework that would enable the entire justice and public safety community to effectively share information at all levels–laying the foundation for local, state, and national justice interoperability.

National Criminal Intelligence Sharing Plan

Developed by the Global Intelligence Working Group (GIWG) and endorsed by Attorney General Ashcroft, the National Criminal Intelligence Sharing Plan ('Plan') is a formal intelligence sharing initiative that addresses the security and intelligence needs recognized after the attacks of September 11, 2001. It describes a nationwide communication capability that will link together all levels of law enforcement personnel, including officers on the streets, intelligence analysts, unit commanders, and police executives for the purpose of sharing critical data.

The Regional Information Sharing Systems™ or RISS, and the FBI's Law Enforcement Online (LEO) systems, which were interconnected September 1, 2002, as a virtual single system, will provide the initial sensitive but unclassified secure communications backbone for implementation of the nationwide criminal intelligence sharing capability. This nationwide sensitive but unclassified communications backbone will support fully functional, bidirectional information sharing capabilities that maximize the reuse of existing local, state, tribal, regional, and federal infrastructure investments. Further configuration of the nationwide sensitive but unclassified communications capability will continue to evolve in conjunction with industry and the development of additional standards, and the connection of other existing sensitive but unclassified networks.

Information-Led Policing (ILP)

Intelligence is worthless unless it can be applied effectively. NIJ's ILP initiative is targeted at enhancing the ability of law enforcement and corrections to prevent and respond to criminal acts by leveraging the Information Technology (IT) revolution. ILP focuses on providing enhanced, web-based incident command systems that use improved information sharing, planning and predictive data mining technologies. It looks to provide seamless exchange of information between disparate information sharing systems and a global reach-back capability from the officer in the street using wireless PDA technology.

ARJIS

NIJ is using the Automated Regional Justice Information System (ARJIS) (www.ARJIS.org) as a testbed for many ILP technologies. ARJIS is a complex criminal justice enterprise network used by 38 local, state and federal agencies in the San Diego region. ARJIS is chartered with supporting a regional web-based enterprise network that uses technical and operational standards to build interfaces to all criminal justice systems in the region. The ARJISNet secure intranet contains data on the region's crime cases, arrests, citations, field interviews, traffic accidents, fraudulent documents, photographs, gang information and stolen property. ARJISNet integrates more than 2,500 workstations and printers throughout the 4,265 square miles of San Diego County. More than 10,000 registered and authorized users are generating more than 35,000 transactions daily. ARJIS is also utilized for tactical analysis, investigations, statistical information and crime analysis. Officers and investigators can additionally request electronic notification when information is obtained by another agency or officer concerning an individual, location or vehicle. The critical success factor for ARJIS is the "single point of entry" to query all regional justice data.

Bomb Squad Information Sharing Network (BSICNet)

This collaborative ILP effort involves NIJ, DHS S&T, the TSWG, the FBI, the ATF, the DOJ Office of the Chief Information Officer (DOJ OCIO), the New York Police Department, the Boston Police Department and the Philadelphia Police Department in the demonstration and evaluation of a real-time information sharing and alert system for bomb squads. It will be a web- and COTS-based system. It will provide real-time information search, sharing and alert to the bomb technician. Ideally, this effort will: employ the FBI's Law Enforcement

on Line (LEO) as its backbone; and will both feed data to and extract data from the ATF's Bomb and Arson Tracking System (BATS). If successful, this limited prototype system will serve as a pilot which will be scalable to provide national coverage. That could be accomplished by agencies accessing to the system on an individual basis—this should not be cost prohibitive for most agencies—or through Federal sponsorship.

Communications Technology (COMMTech)

Communication interoperability remains a major impediment to public safety agencies effective response to major threats to lives and property. Firefighters and emergency response personnel can't always talk. And if they can't talk, they can't respond. The AGILE program was one of the most successful programs of the National Institute of Justice. When interoperability was barely recognized at the national level as a critical public safety concern, AGILE laid a critical foundation for policy development, standards, and technology research that is universally recognized and praised. All of us at NIJ are proud of the role that AGILE has played for law enforcement and all of public safety.

With the establishment of the DHS SAFECOM program, which built upon AGILE's work with the public safety community, NIJ is restructuring its program in this area. We are bringing AGILE to a close, and initiating a new program, called Communications Technology, or CommTech. Unlike AGILE, CommTech will not play a primary role in coordinating the public safety community's interoperability policies or do other work that may be duplicative of SAFECOM's overarching responsibilities. Like AGILE, CommTech will work to inform SAFECOM's policy, coordination, and technology development activities.

NIJ's CommTech program will:

1. Focus on the needs of law enforcement, with a view to all of public safety.
2. Focus on research, development, test and evaluation.
3. Reflect law enforcement's need for improved information sharing and intelligence.

This new program and mission more closely reflect NIJ's role in the scientific and criminal justice communities, thus limiting any confusion among the public and policy-makers. NIJ is reviewing all of its former AGILE work to determine how it does or does not fit within this reorganization.

Standards for Wireless Interoperability and Information Sharing

The long-term solution to public safety interoperability lies in adoption of a national set of standards. SAFECOM has assumed the lead role for the wireless interoperability and information sharing initiative, initiated under NIJ's AGILE program. NIJ continues to participate with SAFCOM in this effort, which is executed in large part at the National Institute of Standards and Technology.

CapWIN

The Capital Wireless Integrated Network (CapWIN) (www.capwin.org) is an NIJ-sponsored partnership between Maryland, Virginia and the District of Columbia to develop an integrated transportation and criminal justice information wireless network. This project will integrate transportation and public safety data and voice communication systems in the two states and the District and will be the first multi-state transportation and public safety integrated wireless network in the United States. The project will have national implications in technology transfer including image/video transmission and the inclusion of transportation applications in an integrated system. National observers will be able to monitor the progress and development of the system during the evolution of the project. This project can potentially build a foundation for networks throughout the United States and other countries. The project will be completed in multiple phases including an initial

strategic planning phase (completed), the implementation phase (underway) and a continuous development and expansion phase.

A pilot test was initiated during the strategic planning phase of the project. The pilot included twenty-two (22) in-vehicle mobile computer systems that allowed messaging between police vehicles in Maryland, Virginia and Washington, D.C.; transportation vehicles in Maryland and Virginia; and local fire vehicles. These mobile platforms and other developmental transportation and public safety systems were successfully interfaced during the pilot project. The primary goal of the project is to have multiple mobile data platforms communicating seamlessly across the network regardless of their jurisdiction or geographical location. These CapWIN end-users will include federal, state and local police, fire, and EMS vehicles as well as state DOT service patrols.

A strategic plan was developed with input from transportation and public safety agencies (federal, state, local) serving the Washington metropolitan area to determine the following: functions needed, system requirements, security requirements, information priorities, evaluation methodology, a multi-year phased implementation strategy, and a long-term business plan that addressed ongoing operations and maintenance.

3. Sensors and Surveillance

Providing law enforcement responders accurate information that they can act on is another high priority technology challenge. Sensors and surveillance technologies can play a key role in identifying terrorists and preventing terrorist attacks. They can also play a key role in effectively responding to a terrorist attack. NIJ is heavily invested in sensors to detect conventional weapons and locate and track individuals in buildings, because these are high priority areas to law enforcement where there has been comparatively little investment by other Federal agencies until comparatively recently. On the other hand, the Institute has invested little effort in detection of WMD materials because of the intense investment in this area by the Departments of Defense, Energy and Homeland Security. NIJ has invested in Biometric technology, despite significant investment by other Federal agencies, principally to focus the technology on law enforcement requirements and to assess it.

Biometrics

Positively identifying an individual has obvious applications to a number of law enforcement functions, including ensuring school safety and combating terrorism. NIJ has funded a number of biometrics technology projects to create a comprehensive program capable of achieving its goals in crime prevention and officer safety for the law enforcement and corrections community. Technology projects have included operational evaluation of portable hand-held digital fingerprint readers; investigation of iris scan technology; various types of biometrics for inmate management; facial recognition; and various approaches to development of a “smart” gun–one that recognizes its user.

NIJ has made a significant investment in facial recognition technology. It funded Analytic Services, Inc. to develop and integrate specialized software search agents into biometric identification modules to find missing children or fugitives on the Internet, in video surveillance, or other large facial databases. Demonstration projects were conducted with the Miami Florida police department and medical examiner’s office, with West Virginia’s State Police Missing Children’s program, and with the U.S. Customs Office Cybersmuggling Center.

Fingerprints and palm prints are now the most relied-upon biometric technology for verifying a person’s identity and positively linking persons to criminal history and other background check records. The potential for expanded use of fingerprints and palm prints for background checks and identifications are currently limited by the technology available to capture the fingerprint friction ridge detail that enables searches of the

databases. New technology with much greater convenience, speed, reliability, affordability, and accuracy must quickly be developed to improve our Nation's ability to meet the screening requirements for criminal, border, transportation, and employment checks.

In 2005, NIJ initiated the Fast Capture Finger/Palm Print Technology program to improve and advance the current state of technology for the capturing of 10 rolled-equivalent fingerprints or fingerprints and palm prints. The resulting technology will allow for the capture of 10 rolled-equivalent fingerprints in 15 seconds or less and both palms in 1 minute or less. This project is a joint effort involving the FBI, DEA, and Justice Management Division within DOJ; and the U.S. Departments of Defense, Homeland Security, and State.

NIJ has in the past, and continues today, to support development of standards and evaluation of biometrics technologies. It funds the National Institute of Standards and Technology to develop evaluation standards and sample data sets for face and fingerprint evaluations. The results of the facial recognition technology evaluations can be found on www.frvt.org.

Weapons Detection

NIJ has the most robust program in the federal government dealing with detection of conventional weapons. Our initial efforts focused on development of improved weapons detection portals. Today, the Institute's focus is on remote detection. NIJ's goal is to provide an affordable technology that will enable its operator to detect both metallic and no metallic weapons, which are concealed on an individual, at a safe distance. Ideally, this technology will be portable and require no cooperation from the subject. Passive systems are preferred because of public perceptions of the potential adverse negative impact of active systems on health. NIJ's efforts have heretofore focused on detecting weapons such as handguns and knives. We are now concerned with detecting suicide bombers as well.

In many ways, being able to detect a suicide bomber is a much easier task that detecting a handgun or a knife. The "weapon," the bomb belt, is much bigger. Additionally, most of the suicide bombs we have seen so far have had a fairly large metal content. The challenge is detecting them at a safe distance, which is much further away than for a handgun.

NIJ is investing heavily in development of passive millimeter wave technology for weapons detection. It appears to offer the ability to both detect suicide bombers at a safe distance as well as smaller weapons. The only commercially available weapons detection technology that offers an ability to detect both metallic and nonmetallic weapons is back-scatter x-ray. Back-scatter x-ray systems have several drawbacks with respect to meeting our goals. They require proximity and cooperation. They are bulky and expensive. They are also active systems.

We think that we are still two to three years away from having a truly functional MMW weapons detection system. While the Institute's efforts are focused on MMW technology, we are open to other approaches. We have ongoing work examining the application of acoustics to this problem and plan to revisit the utility of infrared and radar-based technology.

Although our focus has shifted, NIJ continues to work on improved portal detection technology, particularly in school security applications. Our current efforts focus on reducing the cost and improving the performance of portal systems, with an emphasis on magnetometer-based technology.

Through-the-Wall Surveillance

NIJ also has a very active program in the area of locating and tracking individuals inside buildings. Our work in this area is directed at two objectives. The first is development of a low-cost, hand held "room clearing" system that will enable an office to readily identify if an individual is hiding behind a door or in a room. The

second objective is to provide an affordable, portable system that can be used for hostage rescue situations. This system would provide the incident commander the ability to map internal structures and locate and track individuals within those structures. Ideally, this system will provide an indication of which of those individuals are armed and which are not, and will be able to at least differentiate between hostage rescuers and other individuals. While the room clearing system will work in close proximity to the room being cleared, the hostage rescue system will work remotely.

Radar-based technologies offer the greatest potential across the widest range of building materials, to include reinforced concrete, but are limited by metal walls, or even foil backed insulation. While the Institute's research is focused on radar-based systems, we are exploring alternatives such as acoustics. As with millimeter wave weapons detection, we do not expect to see functional systems that meet our requirements for two to three years.

Concluding Remarks

By far, the largest components of the responder community are state and local public safety agencies. State and local public safety responders will be the first on the scene in the event of a terrorist incident. Working with DHS and other partners such as the TSWG, NIJ has focused its technology efforts in this area on meeting the unmet needs of the law enforcement responder, with emphasis on the technology needs that law enforcement responders share with other state and local public safety agencies. Investment in C3I technologies offers perhaps the greatest potential benefit with respect to improving the capacity of the responder community to respond to a critical incident such as a terrorist attack and save lives and property.