13. Public Safety

In addition to improving the quality of life for millions of people, information technology (IT) in many instances is being used as a tool to actually save lives. IT is used to improve the safety of individuals every day, although many do not realize its importance. Fifteen years ago, efforts to stop crime and terrorism relied on traditional mechanisms: strict physical security at vulnerable facilities, intelligence gathering by government agents, vigilance on the part of all citizens, and a sense of community in which all citizens played a role in protecting each other. These techniques have not been replaced, but nations today have IT as an additional powerful, new tool to ensure public safety.

Much of public safety relies on getting the right information to the right people. Governments use IT to secure their borders against external threats, aid law enforcement in fighting crime, and help communities prepare for, and recover from, disasters. Law enforcement agencies use IT to communicate and share information, monitor and detect crime, and respond to disasters. Finally, IT is at the forefront of the science used by researchers to better understand the complex weather systems that constantly threaten our societies. The IT revolution has given governments the tools, infrastructure, and capabilities to make public safety easier, less expensive, and more effective.

Keeping the Nation Safe

To effectively secure a nation, a government requires accurate information about the individuals and materials entering and leaving the country. As discussed below, IT plays a critical role in securing national borders and managing the flow of people and goods through a country's points of entry. Furthermore, as nations face new threats of terrorism, governments have turned to IT for an array of new tools to detect threats to national security and thwart possible attacks.

Securing National Borders

To prevent unauthorized entry and to facilitate legitimate trade and travel, the United States and other countries increasingly use IT-based tools—including biometric information such as fingerprints, DNA, iris patterns, or facial characteristics and digital photographs—to accurately identify and authenticate both individuals and shipments.

The United States has an IT-enabled system for immigration managed by the U.S. Department of Homeland Security. This program—called US-VISIT—requires all non-U.S. citizens between the ages of 14 and 79 to supply fingerprints and digital photographs when they enter the country or apply for a U.S. visa. These are intended to help in the accurate identification of foreign travelers and in preventing the use of forged or stolen visas. They are shared with the Federal Bureau of Investigations (FBI) and cross-matched against the Department of Homeland Security's watchlist of criminals, immigration violators, and known or suspected terrorists.[1] By the end of 2008, the Department of Homeland Security expects to implement US-VISIT in all U.S. ports of entry.

In the United Kingdom, an e-Borders program similarly collects and analyzes information about individuals entering or leaving the United Kingdom. Under the e-Borders program, airlines, ferries, and rail companies collect electronic information regarding passengers traveling to the United Kingdom and transmit this information to the government to analyze. Data collected in the program are used to coordinate efforts across the government including border patrol, law enforcement, and intelligence agencies.[2] Similar initiatives are being developed elsewhere. In Asia, for example, the Asia-Pacific Economic Cooperation is coordinating an effort to develop an interoperable electronic movement records system. By collecting advanced passenger information for air travel, countries can prescreen passengers before they arrive at the border and have more time to review any possible threats.[3]

The United Kingdom plans to add a biometric component to its e-Borders program to automatically identify individuals at official ports of entry.[4] In fact, the United Kingdom has already implemented a system—the Iris Recognition Immigration System (IRIS)—that allows registered travelers to use biometric identification to quickly enter the country through automated barriers at certain airports, including all five terminals at London's Heathrow Airport. Under IRIS, a camera identifies a traveler from his or her iris pattern; the system then verifies

In the UK, the Iris Recognition Immigration System (IRIS) allows registered travelers to use biometric identification to quickly enter the country through automated barriers at certain airports.

that the passenger has met the entry requirements without requiring any additional passport or visa information.[5]

In recent years, countries in the European Union and the United States have introduced electronic passports—"e-passports"—with biometric information. An e-passport typically contains a radio-frequency identification (RFID) chip, which stores not only the standard passport data but additional digital biometric information such as a photograph, iris pattern, or fingerprint. E-passports help governments better authenticate passport holders and reduce the risk of tampering to these travel documents. The information stored electronically in the e-passport is digitally signed and encrypted to prevent counterfeiting and manipulation. To promote interoperability, most countries use a standard biometric file format defined by the International Civil Aviation Organization. The exact implementation of e-passports varies by country. The only biometric data stored on U.K. e-passports, for example, is a photograph[6]; German e-passports, in addition to including photographs and personal information, contain two fingerprints.[7]

Using biometric-enhanced e-passports, government officials can more quickly and accurately process travelers through customs and immigrations. The Australian government has established SmartGate kiosks at its international airports to allow travelers with Australian or New Zealand e-passport holders to self-process through the passport control area.[8] The SmartGate system uses data in the e-passport and facial recognition technology to perform the customs and immigration checks that are usually conducted by a Customs Officer. SmartGate will be gradually opened to other nationalities that have International Civil Aviation Organization-compliant e-passports.

The demands of physically protecting a nation's border are daunting. In the United States alone, government officials are charged with operating 324 official ports of entry and protecting 5,000 miles of border with Canada, 1,900 miles of border with Mexico, and 95,000 miles of shoreline.[9] IT—particularly in the form of surveillance cameras and sensing devices—plays a key role in providing government officials with the tools they need to secure the borders.

A critical component of the U.S. Department of Homeland Security's comprehensive, multiyear plan to secure U.S. borders and reduce illegal migration launched in 2005—the Secure Border Initiative—is SBInet. SBInet is a comprehensive program whose goal is to field an appropriate mix of state-of-the-art technology and infrastructure and integrate them into a single border security suite for the Department of Homeland Security.[10] The plan is to integrate multiple state-of-the-art systems and sensors, including more expanded use of unmanned aerial vehicles (UAVs), remote-video surveillance camera systems, and sensors.[11] Agents on the ground can use real-time information relayed from radar, surveillance towers, and ground sensors to their satellite phones and handheld devices to track targets on a map and locate unauthorized entries.[12]

Advances in IT have led to the development of UAVs with better remote control, enhanced sensors, and more autonomy. The U.S. Department of Homeland Security uses UAVs to scan remote areas, augmenting ground patrols that lack the manpower and time to reach these areas. UAVs provide precise imagery in real time that enables agents to quickly determine border breaches. One type of UAV—the Predator B—was deployed by the Department of Homeland Security in Operation Safeguard, an experimental law enforcement program conducting missions along the U.S.-Mexican border.[13] The Predator B can fly for 30 hours without refueling, so it can provide sustained coverage over exposed geographic areas.[14] UAVs are also less expensive than manned aircraft. A Predator UAV, for example, costs $4.2 million, whereas a P-3 manned aircraft used for by the U.S. Customs Service for border patrol costs $36 million.[15]

In every nation, customs and immigration officials work to prevent the entry of contraband such as hazardous materials, illegal drugs, and weapons from entering the country. The majority of heavy goods—such as cars, trucks, and appliances—enter the United States in maritime cargo containers. U.S. Customs officials do not have the capacity to inspect every shipment. For that reason, the U.S. Department of Homeland Security has launched its Container Security Initiative. The purpose of this initiative to ensure that cargo containers entering the United States are inspected as early in the supply

chain as possible. With intelligence and information collected in advance (e.g., the cargo manifest), the Department of Homeland Security uses software to automatically identify high-risk containers to target for inspection. Then, rather than waiting for goods to arrive at domestic ports, inspectors use large-scale X-ray and radiation detection devices to examine containers at the port of departure. The Container Security Initiative has been implemented in 58 ports, covering nearly 90 percent of all container traffic coming to the United States.[16] In addition, the Transportation Security Administration of the Department of Homeland Security has created a biometric transportation worker's identification credential, which all individuals must show to enter secure areas at certain ports and on certain vessels.[17]

Screening Cargo and Passengers

Bomb-sniffing dogs are one of the most effective tools for detecting explosives; however, it is not practical to have bomb-sniffing dogs check every person and shipment that enters the country. For that reason, researchers have sought to design electronic devices that will replicate canines' keen abilities.

One such device, funded by the U.S. Defense Advanced Research Projects Agency (DARPA) uses tiny chemically coated sensors called microcantilevers (very small narrow boards) to detect molecules by gauging how they cause surface sensors to bend or vibrate.[18] By analyzing how the sensors behave, scientists can tell how many and what kind of molecules are present. To create a handheld chemical detection system, the company developing the system placed an array of these chemically coated microcantilevers into a device the size of a mobile phone. During tests, the device successfully identified not only explosives but also toxic industrial chemicals and biological threats. DARPA plans to use such devices as mounted sensors inside shipping containers. Transportation Security Administration screeners also could use the devices to screen airline passengers for explosives.[19]

Security officials in the United States and elsewhere have also worked to improve the technology for passenger screening. Some experts have advocated the use of whole-body imaging to detect explosives, plastic weapons, and drugs on passengers that traditional scanners miss. Critics of the current system of screening airline passengers by having them walk through metal detectors and then screening them by handheld scanners, including the U.S. Government Accountability Office, point out that this approach is ineffective against many risks.[20] Whole-body imaging uses backscatter X-rays or millimeter wave technology to give screeners a detailed view of the passenger's body by constructing images from the X-ray photons or radiation reflected by the body. Already such systems have been used in many airports including JFK International Airport in New York, Los Angeles International Airport, and London's Heathrow Airport.

Whole-body imaging essentially provides a detailed view of the traveler's body, and some people object to this as being too invasive. It is nonetheless one of the most accurate way to detect passengers carrying weapons or explosive devices.[21] To address privacy concerns, vendors have introduced a number of controls including a privacy filter that digitally alters the image displayed to the screener to show only the outline of an individual's body. Whole-body imaging devices can also be configured to detect weapons and explosives from a distance of 15 feet to 30 feet, enabling security officials to scan airport lobbies and entrances to subway and rail stations.[22] Eventually imaging systems that use backscatter X-rays or millimeter wave technology may replace metal detectors used for personnel security in other public venues. These imaging technologies can also be used to scan vehicles, cargo, baggage, and mail.

Although security officials focus much of their effort on preventing criminals and weapons from entering the country, they also work to prevent and detect attacks from threats already within the country. Researchers at Purdue University are developing a system to detect and track radiation from nuclear threats—such as a dirty bomb—using a network of mobile phones.[23] Tiny radiation detectors are already commercially available, and although the radiation detection system these researchers are developing would require additional circuitry, the sensors would be small enough that manufacturers could place them in mobile phones, laptops, and personal digital assistants (PDAs) without adding extra bulk. Some mobile phones contain global positioning system (GPS) technology, which would enhance the detection of radiation by precisely locating its source.

Software built into the radiation detection system's network would then evaluate the levels of radiation and its threat. In a recent test, mobile phones with the built-in sensors detected radiation from 15 feet away.[24] The radiation detection system can use data from many different mobile phones to pinpoint the source of the radiation. The main challenge would be achieving a high enough rate of adoption of devices with the sensors, either voluntarily or by mandate, for the system to provide an effective layer of protection.

Analyzing Large Sets of Data for National Intelligence Information

Investigators have found that intelligence officials often had evidence of an impending attack prior to a terrorist strike but failed to connect the dots in time to prevent the attack.[25] IT provides government officials valuable tools to efficiently analyze large sets of data and derive useful intelligence—intelligence that may allow officials to detect terrorist and criminal activity in time to do something about it.

One way that IT helps government analysts connect the dots is by making it possible to share information quickly. In 2007, the Central Intelligence Agency in the United States introduced Intellipedia. Much like the user-built, Web-based encyclopedia Wikipedia—built with Wiki software designed to enable anyone who accesses it to contribute or modify content—Intellipedia allows analysts from different departments to post, read, and edit information on security intelligence. Intellipedia also has other Web 2.0 features such as photo and video sharing, content tagging, blogs and RSS feeds. Each entry in Intellipedia is organized by topic, not by corporate structure, and this organization allows the contributors to act like "a community of analysts rather than a community of agencies."[26] Such a medium helps spread ideas from "base camps of knowledge" across traditionally departmentally demarcated lines of jurisdiction.[27]

Recent advances in IT have allowed government and other investigators to make use of a special form of data analysis known as data mining. Data mining uses computerized analysis, including statistical modeling, mathematical algorithms, and machine learning techniques, to derive patterns and relationships from data. In contrast to standard data analysis, which may only seek to prove or disprove a hypothesis provided by the user, data mining generates hypotheses that the user must then verify.[28] Thus, for example, a data-mining program might discover that an individual has a relationship to an extremist organization or matches the profile of a known terrorist; however, an investigator must still determine the validity of the match.

U.S. government officials have used data mining for a wide variety of objectives, including monitoring financial transactions and preventing terrorists from obtaining financial support. The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) investigates terrorist financing and money laundering using activity reports filed electronically by financial institutions. Law enforcement agencies can access FinCEN financial data directly over a secure Internet connection.[29] Financial institutions also search their accounts for potential matches to names on government investigative lists and notify FinCEN if they find a match.[30]

The CIA has introduced Intellipedia, a Web application which allows analysts from different departments to post, read, and edit information on security intelligence.

Other countries have made similar efforts to stop terrorist financing and prevent money laundering. In Germany, the Federal Criminal Police Office monitors suspicious financial activity and reviews electronic databases to ensure banks comply with antiterrorism laws.[31] Australia has also launched similar initiatives through its Australian Transaction Reports and Analysis Centre (AUSTRAC), which is an anti-money-laundering and counterterrorism financing organization. The Data Mining and Research Unit of AUSTRAC uses data-mining techniques to proactively and reactively analyze and monitor finance transactions to uncover hidden patterns.[32] In addition, the Office of

National Security in Australia has funded antiterrorism grants to develop enhanced data-mining tools.[33]

Data-mining efforts have led to the capture of suspected terrorists. Following the 9/11 attacks in the United States, the U.S. Department of Treasury worked with the Central Intelligence Agency to gain access to financial records from Swift, a Belgian banking cooperative that processes more than 11 million transactions a day between 7,800 financial institutions around the world.[34] Armed with this financial data, government investigators have discovered ties between known terrorists, domestic terror cells, and the extremist groups financing them. As an example, government investigators' analysis of data from Swift led to the capture of Riduan Isamuddin, the suspected mastermind of the 2002 Bali resort bombing.[35]

To use data mining, government agencies must be able to share data. Governments around the world have launched multiple data-sharing tools to improve collaboration between their law enforcement agencies and to share data on investigations and criminals. In Germany, for example, government groups have come together to develop a central database of extremists suspected of terrorism to improve coordination between law enforcement agencies.[36] In the United States, the FBI now can access data from multiple sources via the Investigative Data Warehouse (IDW), which combines data from the FBI's records and criminal case files with information from the U.S. Treasury Department, State Department, and Department of Homeland Security. Launched in 2004, the IDW saves significant time and effort for FBI agents, who can use it to complete a search of a thousand names of potential suspects in 30 minutes.[37] An equivalent search without the IDW would require FBI agents to query 15 different databases and waste thousands of hours of time. IDW allows FBI agents to link and cross-match names, Social Security numbers, and drivers' licenses across hundreds of millions of records.[38]

Preventing and Detecting Crime

Beyond playing a role in protecting the homeland against terrorism and external threats, IT plays a key role in ensuring public safety from domestic threats such as crime. Law enforcement agencies focus a large part of their efforts on proactive initiatives intended to prevent and detect crime. To be effective, agencies must thoroughly understand their community and the nature of crime within their jurisdiction. IT provides law enforcement with tools to capture, analyze, and present this information in a meaningful format. In addition, IT automates many of the time-consuming tasks associated with police work and frees police resources to be used on other effective programs. Some police departments have been quick to adopt technology to help their officers in the field. In the United States, the police department in Alexandria, Virginia, began giving its officers wireless handheld computers as early as 1997 so that they could access and report important information while on patrol, on a stakeout or at the scene of a crime.[46] Police officers of the future will be just as likely to carry a computer as they will to carry a gun.

Remote Monitoring

Law enforcement officials use various forms of remote monitoring as a tool to reduce crime and rehabilitate offenders. Remote monitoring acts as a deterrent because offenders know that they will be caught if they commit a crime or violate their parole. Police can also use remote monitoring to investigate crimes and eliminate suspects who can provide an electronic alibi. In addition, communities save money by using remote monitoring of offenders as an alternative to more expensive punishment such as incarceration while also allowing offenders to become productive members of society.

One form of remote monitoring uses global positioning system (GPS) technology. Law enforcement officials can use tamper-resistant GPS-enabled devices to track the movements and location of offenders sentenced to house arrest. Police and parole officers can either track individuals in real time using GPS-enabled devices (such as ankle bracelets) with transmitters or create a time-stamped log for later review with passive devices. Using GPS devices for remote monitoring can reduce expenses and improve outcomes for the criminal justice system. Such monitoring provides an effective means of enforcing house arrest, even for sentences that allow certain authorized activities away from the home. Rather than being put in jail, some low-risk offenders can

Box 13-1: IT and the Fight Against Human Trafficking

Modern-day slavery takes a horrifying toll on its victims—primarily women and children—who suffer loss of liberty, physical and emotional abuse, and sometimes even death. Human trafficking claims millions of victims every year and contributes to organized crime and global health risks.[39] IT serves as an important tool to combat this cruel practice.

IT has provided an effective medium for modern-day abolitionists to organize, communicate, and raise awareness. A multimedia campaign produced by the MTV Europe Foundation that works to increase awareness and prevention of human trafficking through its television programs, online content, concerts, and media events, for example, is MTV EXIT. The program's Internet site helps at-risk young adults in Asia learn how to stay safe and report abuse, and connects teenagers in European countries and other parts of the world with organizations they can get involved with to end human trafficking. MTV EXIT reaches 300 million households in 25 different countries and is translated into 10 different languages.[40]

A number of IT initiatives to increase information sharing and coordination among antitrafficking nongovernmental organizations, government organizations, and other groups in southeast Asia have been supported by the Asia Foundation, itself a nongovernmental organization.[41] One such initiative is building a human trafficking Web portal to link the different antitrafficking organization throughout Thailand, Cambodia, and Laos. Nongovernmental organizations working in rural areas track missing persons, while nongovernmental organizations working in cities, which are often the destination of trafficked persons, maintain lists of victims seeking help. More information sharing between these groups could help resolve missing person cases and help victims of trafficking contact their families. Using a single, comprehensive missing persons website allows nongovernmental organizations to be more effective and find local organizations to help victims adjust when they return home.[42]

Another antitrafficking project in southeast Asia is the United Nations Educational, Scientific, and Cultural Organization's (UNESCO) Social Sentinel Surveillance Project. This project is linked to a geographic information system (GIS)—an information system for capturing, storing, analyzing, managing, and presenting geographically referenced information. The Social Sentinel Surveillance Project trains villagers, local nongovernmental organizations, and health workers in China, Myanmar, and Laos to collect and report information on the migration of local women and children in their community at risk for trafficking. Similar data are collected from interviews with sex workers in Thailand, and all of the data are geocoded. Thus, researchers can use a GIS program to analyze the data and better understand how victims are trafficked, to understand migration patterns, to predict areas of high risk based on socioeconomic factors, and to determine which interventions are most effective.[43]

Nongovernmental organizations need reliable data to raise awareness and convince policymakers of the need to direct resources to the problem of human trafficking. Unfortunately, because of mistrust between communities and law enforcement, victims may be reluctant to report trafficking. In Cambodia, the Cambodian Women's Crisis Center is developing a database to collect and track information on the nature and scope of trafficking.[44] Similarly, the International Organization for Migration collects data on the victims it assists in the Counter-Trafficking Module Database. UNESCO has created a Trafficking Statistics Project website with the goal of assembling a comprehensive database of trafficking statistics and their corresponding methodologies.[45]

be required to stay at home, except to go out to work where they can make money to help pay for victim restitution. The cost of incarceration can cost a state approximately $25,000 per inmate per year, whereas the cost of remotely monitoring an inmate can cost less than $5,000 per year.[47] GPS-enabled devices also help monitor high-risk offenders. Law enforcement can use a computer to draw exclusion zones for sex offenders so that an alert will be sent out if the offender enters a restricted area such as a playground or school. GPS devices can similarly be used to enforce restraining orders. Thus, for example, if domestic violence offenders violate restrictions on visiting their spouse at their home or place of work, the police will be notified in real time.[48]

Law enforcement officials have turned to other electronic devices to monitor offenders with substance abuse problems. Many alternative sentencing

programs require participants to cease using drugs or alcohol for the duration of their rehabilitation program. Traditional drug and alcohol testing involves supervised urine collection which must then be sent to a laboratory for analysis. There are new technologies that provide a more cost-effective alternative to this approach. One example is an alcohol-testing device that uses near infrared spectroscopy to measure an individual's alcohol level by examining a subject's inner forearm. Unlike traditional alcohol testing, this testing device can be used without supervision because the device uses biometrics to authenticate each person during the reading.[49] Another technology that counties in California have used to ensure that offenders in diversion programs are attending drug treatment counseling and parole meetings is a small plastic card embedded with the defendant's pertinent treatment information. County judges can easily monitor which offenders are meeting their obligations and which ones are not.[50]

Other IT-enabled devices can be used to make it harder for at-risk offenders to engage in criminal behavior. Although offenders' driving privileges are often suspended or restricted to reduce their threat to the community, studies have found that as many as 75 percent of all drivers with suspended licenses continue to drive.[51] Ignition interlock devices can prevent individuals from driving their cars if they have been drinking. An ignition interlock device requires the driver to blow into the device before starting the car; if the device detects a blood alcohol concentration in the driver above a certain threshold, then the car will not start. To help prevent cheating, the device continues to request additional samples from the driver at random intervals. An ignition interlock device also can be a useful tool to allow offenders to regain their driving privileges. In Ontario, for example, all individuals convicted of an impaired driving offense are required to have an ignition interlock device installed on their personal vehicles for a minimum of one year to retain their driving privileges; such individuals must pay for the cost of the device and bring the vehicle in for routine inspections.[52]

Other forms of remote monitoring are red light cameras and speed sensors to combat unsafe driving practices such as running red lights, speeding, and aggressive driving. Red light cameras have been deployed at dangerous rural and urban intersections to help reduce accident rates. Studies have found that equipping intersections with such cameras results in a decrease in right-angle crashes, accompanied by a fairly equal increase in rear-end crashes. (The increase in rear-end crashes may result because drivers are more likely to stop at a red light when it is equipped with a camera.) The net benefit of installing red light cameras is positive, however, because the injuries from rear-end crashes tend to be less severe than injuries from right-angle crashes.[53] In fact, using red light cameras reduces the total number of crashes with injuries by 25 to 30 percent.[54]

Remote-monitoring systems such as red light cameras and speed sensors to combat unsafe driving practices such as speeding and aggressive driving are important for two reasons: they stretch public safety funds further since police do not have to be engaged in this kind of routine work and they make people more aware that they will be more likely to be fined if they violate traffic laws. Government officials design smart traffic system not just to be punitive but also to promote safe driving.

Many remote-monitoring technologies target speeding. One in three traffic fatalities in the United States occurs because of speeding, and annually more than half a million people are injured.[55] Technologies like variable speed limit signs can automatically adjust the speed limit according to traffic flows, adverse weather conditions, or the presence of construction workers to improve driving safety.[56] In Herndon, Virginia, a speed-detection unit is connected to a traffic signal, so that if a vehicle is speeding, then the traffic signal will turn red; a street sign provides drivers advanced warning so they know that speeding will not get them to their destination any faster, thus promoting safer driving behavior.[57]

Digital Video Surveillance

For many years, law enforcement officers have used video surveillance—typically in the form of analog closed-circuit television (CCTV) cameras—to remotely monitor public places. Recently, however, police departments have been able to take advantage of the low cost of digital video cameras and wireless networks to develop large-scale, network-enabled video surveillance systems that allow officers to monitor high-quality video feeds and control multiple surveillance cameras in real time from a remote

location. Wireless video cameras serve both as a deterrent to crime and as a tool for detecting and investigating crimes. Police departments can take advantage of the wireless cameras' portability and easily move the cameras to new locations to target crime hotspots. The initial results from many of these Internet Protocol (IP)-based video surveillance systems have been impressive. In Dallas, Texas, for example, the police department installed 40 IP-based digital video surveillance cameras in the city's central business district. The Dallas police department reported a 12 percent drop in crimes and a 9 percent increase in arrests in the first year after implementation of the system.[58]

There have been several high-profile projects that combined face-recognition systems with video surveillance to automatically identify individuals in a crowd, including projects at Boston Logan Airport, Keflavik Airport in Iceland, and the 2001 Super Bowl XXXV in Tampa, Florida. The objective with these systems was to have the CCTV cameras capture faces in a crowd so that they could then be matched to a database of known terrorists, criminals, and other wanted individuals. The projects had mixed success. In Tampa, the police department identified 19 people at the Super Bowl with outstanding warrants; however, it later decided to scrap a larger neighborhood surveillance program because the program did not make one match during a two-year pilot test of suspected criminals and runaway children.[59] In a three-month test of the system at Boston Logan Airport, the system correctly detected volunteers 153 times but failed 96 times.[60] Other airport trials combining face-recognition systems with video surveillance yielded similar results or were abandoned because of a high rate of false-positives.[61] Nevertheless, researchers expect performance of such systems to improve as the technology advances.

One of the largest deployments of CCTV cameras deployed throughout the nation, with over 4.2 million cameras, is in the United Kingdom.[62] In Birmingham and parts of London, British police have added face-recognition technology to CCTV systems to help combat crime. Although tests have found that the face-recognition technology failed to detect individuals on an alert list, the systems themselves have served as a deterrent to crime, and crime rates have dropped as much as 40 percent.[63] The CCTV systems were used by British investigators to investigate and identify the terrorists involved in the 2005 London subway bombings.[64] They have also provided valuable evidence to prosecute individuals accused of plotting to bomb the London subway.[65]

The police in the United Kingdom have extended the capabilities of video surveillance by adding automatic license-plate-recognition technology to track vehicles' movements. As digital cameras snap photographs of cars in transit, a computer logs each vehicle's license plate number along with the time, date, and location. A computer can then crosscheck these vehicles against police databases to verify that the vehicle has not been stolen, its tags are up to date, and it has insurance. Police expect the central database to be able to process up to 100 million plates per day.[66] Police in Seattle, Washington, use a similar technology in car-mounted cameras that alerts police officers if a nearby vehicle is stolen or on a watchlist. These cameras are capable of processing up to 1,000 license plates per hour.[67] The results can be dramatic: in 2007, a police officer in San Jose, California, arrested a suspect for kidnapping and forcible child molestation after his automatic license plate recognition system alerted him that the vehicle was stolen and used to kidnap a 12-year-old girl a day earlier. Had the system not been in place, the officer would probably never have stopped the suspect.[68]

Red light cameras have been deployed at dangerous rural and urban intersections; using these cameras reduces the total number of crashes with injuries by 25 to 30 percent.

Better Crime Analysis

IT allows police departments to better understand crime trends, manage their staff and resources and engage with their community.[69] Police departments of all sizes have adopted the CompStat manage-

ment approach pioneered by the New York Police Department (NYPD). They use IT to collect and analyze crime and police data, then report on trends to gain better intelligence about crime and resource utilization. CompStat helped the NYPD implement its "broken windows" theory of policing that small crimes lead to big crimes. The CompStat method generates clear metrics that police department chiefs can use to hold police managers more accountable for their performance, validate the effectiveness of enforcement tactics, and rapidly respond to emerging crime trends.[70] Furthermore, by using CompStat in combination with an effective policing strategy, police departments can target specific areas that are hotspots for crime.

One important tool used by police departments that have adopted CompStat is crime mapping using GIS technology. Police departments process large amounts of data, with large departments processing thousands of crime incident reports every year, and the amount of data can be overwhelming. Although data from sources such as crime reports provide critical information, police departments need tools to manage the flow of information. Crime mapping uses IT to help police officers process crime incident reports by creating a visual representation of the crime committed within a certain geographic area over a certain time period. When police officers start a new shift, therefore, they can quickly review a map of recent crime incidents from their jurisdiction.[71]

Police use crime mapping software to process crime reports and create a visual representation of the crime committed within a certain geographic area over a certain time period.

Other available GIS applications can be used by police departments to conduct temporal and spatial analyses of crime data to identify trends, track serial offenders, and target hotspots for crime prevention. A prime example is CrimeStats, a spatial statistics software program developed by the National Institute of Justice, the research arm of the U.S. Department of Justice, and made available for free to police departments and researchers. Using CrimeStats, police can better identify high-crime areas and conduct geographic-profiling to target serial offenders.[72]

Some police departments use gunshot locator systems to automate the reporting of gunshots and to combat gun-related crime. Many times, gunfire goes unreported by citizens, especially those who have become accustomed to the noise. Yet gun-related crime affects the public safety of many communities. In 2004, 66 percent of the homicides in the United States were committed with guns.[73] The core of the gunshot locator system is a network of wired and wireless sensors spread across a city or along a highway. When gunshots are fired, the system can analyze the acoustics to determine the precise location of the shooting and even the direction the shooter is moving. The sensing system is integrated with mapping tools to provide law enforcement real-time visual information about gunfire within a certain geographic area. When gunshots are fired, the system immediately transmits this information to a response center, allowing police to respond within minutes. The real-time alerts provided by gunshot locator systems improve the ability of police to arrest criminals and provide medical aid to gunshot victims. After installing a gunshot locator system in Los Angeles County, the sheriff's department found that citizens were reporting only about 11 percent of gunfire that occurred. The information provided by the gunshot locator system allows police departments to better patrol gun crime hotspots and to target these areas with antigun programs.[74]

Responding to Crime

Communities want safe neighborhoods with low crime rates, and they have overwhelmingly turned to IT for solutions. When criminals strike, police need the tools necessary to provide an effective response. By using IT, a police force can be more productive, solve more crimes, and better protect the lives and property of the public. Law enforcement agents rely extensively on IT for criminal investigations, hazard-

ous operations, and communication networks.

Biometrics and DNA in Law Enforcement

Biometric information for uniquely recognizing humans based upon one or more intrinsic physical traits includes fingerprints, images of the face, iris and retina, voiceprints, and DNA. Criminal investigators have long relied on biometric measurements such as fingerprints to identify suspects using evidence from a crime scene. Such information has served investigators in two ways: allowing them to verify that a known suspect was at the scene of a crime and helping them identify suspects on the basis of biometric evidence found at the scene.

In recent years, IT has taken biometric identification to an entirely new level. Using programs such as the Automated Fingerprint Identification System, for example, investigators can collect a set of fingerprints at a crime scene electronically using a mobile device and then compare them against a database of millions of fingerprints within seconds. Furthermore, biometric data such as fingerprints, images of the face, iris, and retina are increasingly collected by governments when they issue identification cards or passports. Consequently, criminal investigators now have national and international databases of digital biometric data at their disposal to search for and identify suspects.

For convicts, some countries collect biometric data such as DNA samples, which are more information-rich (i.e., have more distinguishing characteristics) than other biometric identifiers.[75] The United Kingdom, for example, has established a national DNA database, and police can collect DNA samples from any individual arrested for a crime just as they can collect fingerprints and mug shots.[76] France is working on a similar project to establish a national DNA database to track and identify terrorists and criminals.[77]

DNA has become an important link in the criminal justice system to solve crimes, identify missing persons, and protect the innocent. In the United States, for example, there have been 155 post-conviction exonerations using DNA evidence since 2000.[78] In addition, DNA can help law enforcement solve "cold" cases, thereby helping catch criminals who have managed to escape justice. New technology allows investigators to generate DNA profiles from existing evidence; and growing DNA databases give law enforcement officials a better chance of catching the criminal.[79] This approach helped identify the perpetrator of a series of brutal attacks and murders in North Carolina that had gone unsolved for over a decade. At the time of the crime, forensic DNA evidence indicated all of the crimes were committed by the same individual, but the police did not have any suspects. Ten years later, the police found a match to the DNA collected at the crime scenes after taking a routine DNA sample from an individual arrested for a shooting incident. When confronted with the DNA evidence, the suspect confessed to the attacks, thereby solving the case.[80]

Making it more difficult for criminals to assume false identities or fraudulently obtain government identity cards makes it easier for law enforcement officials to solve crimes and track criminals. Many governments and organizations have adopted IT to produce more secure identification cards to reduce the risk of fraud and forgery. As previously noted, many governments are now using e-passports to help secure borders. In addition, many governments have adopted sophisticated national or state identification smart cards that store biometric information such as a digital photograph, fingerprint, or retinal scan that makes it possible to definitively associate a particular person with an identity (name, date of birth, passport number, etc.). Imposters cannot conduct fraudulent transactions with a stolen ID card with biometric information, and criminals cannot assume fake identifies because their biometric signature will not match the one stored on the card.

The world's first smart national ID card is the MyKad developed in Malaysia. Developed by several agencies, including the Malaysian Road Transport Department, the Royal Malaysian Police, the Immigration Department, and the Ministry of Health, Malaysia's compulsory national ID card is designed to be a single authentication token for use in transactions with both government entities and private businesses.[81] Each smart ID card contains encrypted information about its owner, including e-cash balance, health information, driver's license information, passport information, and biometric data including fingerprints and a photograph. Malaysian citizens and permanent residents can use their smart ID card for many applications, including e-com-

merce transactions, e-banking, health care, and the use of public transportation.[82] Hong Kong has issued smart ID cards since 2003.[83] Spain moved to electronic IDs with biometrics in March 2006. For Spain, one of the principal goals of moving to electronic IDs was to create a secure platform for electronic signatures for everything from e-government to e-commerce.[84] Using electronic signatures allows individuals to complete legally binding transactions online (e.g., to sign a tax return).

Robotics in Law Enforcement

Law enforcement agencies use IT-enabled robots for a variety of tasks to assist officers and reduce their exposure to hazards. IT-enabled robots can be used by special weapons and tactics (SWAT) teams and bomb squads in dangerous operations to reduce the risk to human life. Law enforcement agencies around the world use robots for surveillance, the handling of hazardous materials, and bomb disposal. Law enforcement agents in the United Kingdom, for example, have relied since the 1970s on robots for bomb disposal in combating violence in Northern Ireland.[85] Robotic technology continues to advance and today's robots are portable, battery-powered wireless devices equipped with video cameras, microphones, and remote-controlled robotic arms. In fact, today's robots can climb stairs and curbs, open car doors, inspect under vehicles, and safely detonate explosives.[86]

Crime Scene Mapping

Crime scenes provide valuable information to help investigators solve crimes and prosecute cases. In the past, investigators have had to rely principally on two-dimensional drawings and photographs of crime scenes. A new technology called high-definition surveying relies on lasers and digital cameras to rapidly construct a detailed, three-dimensional computer model of a crime scene or accident. High-definition imaging systems provide two main benefits: they help investigators solve crimes and determine fault, and they help prosecutors explain a crime to the jury. The imaging systems work automatically: investigators set up the device in the middle of the crime scene, and the system automatically scans the surrounding environment. The imaging systems can be used indoors or outdoors, regardless of the amount of visible light, for surveying environments as small as an apartment or as large as a city block. Using such an imaging system, investigators can see exactly where evidence was found, zoom in on different locations, and manipulate the viewing angle to see the scene from any perspective. Thus, for example, a prosecutor can show members of the jury exactly what a witness would have seen looking into a building from the outside. Investigators can also create forensic animations to reconstruct a crime to better visualize a sequence of events.[87]

Empowering Communities and Victims of Crime

Police departments use a variety of IT-based tools to empower communities and victims of crime. In addition to using crime mapping for internal operations, police use crime mapping to share information about crime with the public. In Portland, Oregon, for example, the police department created a public version of its interactive crime-mapping tool and made it available to the community on a website. Citizens can use the website to generate maps of crime reports from the past 12 months; they can also sign up to receive custom alerts when certain crimes are committed near a given address. Police departments use crime-mapping tools on the Internet to alert the community to crimes, engage the public in solving problems, and ensure accountability for public safety efforts.[88]

Other IT-enabled tools are used to alert community members to possible threats, such as from likely repeat offenders. As an example, many communities require sex offenders to register in public databases so neighbors can remain vigilant against any dangers and take any necessary precautions. In addition, as of 2008, 34 states in the United States have some type of a statewide, automated victim notification system.[89] Victims and witnesses of a crime can register on such systems to receive alerts about the status of a particular inmate. IT-enabled victim notification systems make it easier for victims to be notified when an offender is released, transferred, or escapes from jail so that they can take steps to protect themselves. Such systems also offer psychological comfort to victims because they know they can access the state's prison inmate database online and reassure

themselves that a particular inmate is still in jail.

Making Law Enforcement More Transparent

Using IT, government can make many aspects of law enforcement more transparent. Beyond allowing law enforcement officials to collect and analyze large amount of data, IT also allows this information to be shared with the public. Police departments that have computerized their incident and arrest reports can more easily share their data with nonprofit organizations and journalists. Using these data, researchers can monitor police performance and analyze the data for evidence of impropriety such as racial profiling. One city newspaper, for example, analyzed 480,000 incident reports from the Toronto Police Service's Criminal Information Processing System and reported evidence of racial profiling for certain charges and harsher treatment for offenders based on race.[90] Sharing data on incidents and arrests to the public can help police departments end improper practices and thereby build trust in the community.

Many police departments use electronic audio and video recording to create more transparency in the criminal justice system. Electronic recordings of police interrogations can provide valuable evidence to ensure the conviction of the guilty and provide an objective record. Studies have found that as many as 25 percent of false convictions can be at least partially attributed to wrongful confessions.[91] Electronic recordings can help protect the innocent and ensure that the true criminals are punished, help defend police against false accusations of impropriety, and help ensure justice for victims of police brutality.[92]

Although police departments have used video and audio records for many years, the recent move to digital video allows greater and more effective use of video technology. Digital video allows law enforcement officers to easily catalogue, archive, and share evidence among investigators. As an example, multiple police officers can monitor live streaming video of a police interrogation from their desktop computers or quickly access previous police tapes to review evidence. In addition, given the ever-increasing storage capabilities of today's computers, police departments can more easily store large amounts of digital video. This means that police departments can deploy video cameras widely throughout their operations. The use of car-mounted digital cameras, for example, ensures that citizens have a record of police encounters and can help improve community relations between police departments and the residents they protect.[93]

Finally, the IT revolution has equipped citizens with new tools to improve accountability in law enforcement. With so many cell phones now equipped with digital cameras, when a crime occurs witnesses are more likely to be able to provide digital evidence. Countless examples abound on the Internet of individuals who recorded questionable police action via a digital camera. In 2006, three separate incidents in Los Angeles were caught on video by ordinary citizens during a single week showing alleged police brutality.[94] Website like YouTube and CNN's iReport allow any individual with a camera to quickly share a video or photographic record with the media and the public.

Facilitating Emergency Communications

During an emergency, robust, flexible, mobile communication is essential to enable first responders such as police, fire, and emergency medical services to communicate with other emergency workers and coordinate their response. Unfortunately, many existing communications networks, including cellular phone networks, do not offer enough bandwidth or reliability for emergency communications and can be overloaded by subscribers during an emergency. Challenges related to interoperability can hamper interjurisdictional emergency response efforts. And good communications networks in rural areas may

High-definition surveying relies on lasers and digital cameras to rapidly construct a detailed, three-dimensional computer model of a crime scene or accident.

be destroyed during an emergency or nonexistent.[95] IT is helping to address these issues.

Public Safety Networks

To help their communities better prepare for an effective emergency response to accidents and natural disasters, many municipalities have developed state-of-the-art, regional public safety networks to protect the lives of first responders and the citizens they serve. Many technologies can be used for creating public safety networks including cellular, municipal wireless, satellite and existing analog television spectrum.[96]

Public safety networks enable public safety workers to use traditional voice communication but also allow them to access online resources and connect network-enabled devices. Thus, for example, police officers on patrol can use a wireless network to access the FBI's National Crime Information Center in the field to look up in real time fingerprint records, mug shots, and criminal histories.[97] Similarly, police officers can connect to their local police department network to complete routine tasks such as submitting crime reports and issuing traffic citations. Firefighters can use public safety networks to check traffic patterns and find driving directions on the way to a fire. Also important to firefighters is the availability of electronic building plans. Companies such as BeSafe Technologies work with schools, governments, corporations, and residential communities to pull together—and when necessary generate anew—all the relevant information about buildings (floor plans, location of utility boxes, entries, etc.), then make that data available through an online interface accessible to emergency personnel. That way, when an emergency happens, the first responders will have all the information they need to know about a building, including real-time information like which fire alarms were set off, so that they do not have to enter a potentially dangerous situation blindly.

One pilot project in the United Kingdom demonstrated the benefits of a broadband mobile network for public safety. Using existing cellular networks, officers could access the police department network and stream video to headquarters.[98] In the United States, cities including Portland, Oregon, have achieved high levels of reliability and scalability in their public safety networks by using the architecture of a wireless mesh network. Wireless mesh networks use many nodes that act as both an access point for clients and part of the backend network routing infrastructure. This architecture is highly resilient to node failures, for example from bad weather, and allows city planners to easily increase capacity to meet new demand by adding more nodes. In addition, mesh networks can use network management techniques to ensure quality of service levels in an emergency for high-priority network traffic.[99]

The rise of Internet-enabled cameras has also enabled first responders to access more information when responding to emergencies in buildings because they can see what is happening on the ground even before sending in the initial team to determine the appropriate response and where the trouble areas are. Furthermore, the growing prevalence of high-bandwidth wireless connectivity means that such cameras can be accessed while on the move from inside police cars, firetrucks, and ambulances.

Police officers on patrol can use a wireless network to access the FBI's National Crime Information Center in the field to look up fingerprint records, mug shots, and criminal histories.

The Emergency Alert System

The Emergency Alert System (EAS) is a national public warning system in the United States that was put into place to give the U.S. president the ability to communicate with the American public in the event of a national emergency. State and local officials can use the EAS to address emergencies in their specific areas. Because traditional two-way communication networks can quickly become overloaded in a major emergency, the government must rely on broadcast networks to communicate with the public. The EAS is a public warning sys-

tem for all broadcasters, including television, radio, and cable and satellite services. To allow the secure transmission of alerts in various formats, including text, audio, and video, the Federal Communications Commission (FCC) has defined a special messaging protocol to use on the EAS.[100] The FCC requires all participating broadcasters to have dedicated equipment that will automatically receive, decode, and retransmit messages sent through the EAS. It also requires that all EAS equipment be tested weekly. The National Weather Service uses the EAS to distribute emergency weather information to the public, and state and local officials use the EAS to distribute local emergency information.[101]

Currently, one important use of the EAS is to help locate missing or abducted children. State and local law enforcement can use the emergency alert system to broadcast an AMBER (America's Missing: Broadcasting Emergency Response) Alert to law enforcement and the media about a child abduction. The AMBER Alert system facilitates the rapid distribution of information on a child abduction to the public so members of the community can assist in the search and recovery of the child. AMBER Alert information includes descriptions of the child, abductor and any information about the abductor's vehicle. Television and radio stations voluntarily alert their audiences to the information and electronic highway billboards display the alerts for drivers. All cell phone subscribers can also register to receive geographic-specific AMBER Alerts as text messages on their cell phones.[102]

A new initiative, AmberView, would provide a tool to broadcast an abducted child's image to law enforcement, the media, and the public. Through this initiative, on the annual school picture day, parents can consent to having a high-quality digital photograph and updated biographical and physical information about their children stored in a secure database. In the event of abduction, law enforcement officials can use the digital image in this database to quickly distribute the missing child's photograph.[103]

The next generation of EAS is the Integrated Public Alert and Warning System (IPAWS), which will allow the transmission of alerts through multiple devices, including cell phones, pagers, radio, personal digital assistants (PDAs), road signs, and personal computers. IPAWS will also allow alerts to be sent in a variety of formats and languages, including in American Sign Language and Braille.[104]

Other Emergency Communications Systems

Enhanced 911. IT is especially vital to the communications networks that are the key to a successful emergency response to accidents and natural disasters.[105] In the United States and Canada, IT is used in location technology that enables emergency services to locate the geographic position of the caller—called enhanced 911 (or e-911). E-911 automatically associates an address with the caller's phone number and directs the call to the nearest Public Safety Answering Point (a county- or city-controlled agency responsible for answering 9-1-1 calls for emergency assistance from police, fire, and ambulance services). The dispatcher sees the caller's address immediately, saving the precious time it used to take to recite and enter that information and overcoming situations where the caller may be unable to provide their address because they do not know it or are distracted by the emergency.[106] This basic concept of e-911 has expanded into a second phase that uses either triangulation between cellular towers or the GPS capabilities built into many mobile phones to do the same routing for mobile callers. Thus, e-911 allows emergency personnel to find callers wherever they might be.

Websites and Wikis. IT also empowers communities to organize and respond to emergencies and natural disasters. Many communities have used the Internet during an emergency to coordinate recovery efforts and match the many individuals requesting aid to offers of assistance. After Hurricane Katrina hit Louisiana and Mississippi in the summer of 2005, websites such as Craigslist provided each community an open forum to exchange ideas and information. Animal rescue organizations used the Internet to locate pet owners, find new homes for animals, and reach out to donors. Volunteers working around the world established the KatrinaHelp Wiki as a clearinghouse for information on multiple recovery efforts. One major initiative, the Katrina PeopleFinder project, aggregated data about survivors from multiple sources into a single repository using an interoperable XML standard called the

People Finder Interchange Format. Volunteers could sign up to manually input data into the repository from unstructured data sources gathered by relief agencies, newspapers or employers. By harnessing the power of the Internet, volunteers were able to quickly enter data for over 640,000 Katrina survivors.[107] Family and friends could then search this database to find missing loved ones.[108] Other projects on the wiki helped victims find shelter, access health care, receive government assistance, and find jobs.[109]

Microblogging. Microblogging is another IT-enabled tool to help disseminate information during emergencies and natural disasters. Services such as Twitter allow users to post short messages about their activities. Although originally built as a tool for friends to keep in touch, Twitter has introduced a new avenue for finding information in real time. Thus, for example, during emergencies like the California wildfires and the earthquake in China, Twitter has proven its worth as a resource for real-time information. In China, news of the earthquake hit Twitter even before the U.S. Geological Survey, which is charged with giving early warnings about earthquakes, had any information on its website.[110] In California, when local news was overwhelmed and national news could only provide scant details, residents turned to Twitter for information about evacuations, meeting points, and places to gather supplies.[111] In both instances, because locals were microbloggers, an organic network of news gatherers came into being, providing real-time updates of what was actually happening on the ground, helping people react in the safest possible way and, by coordinating response efforts, likely saving lives.

Text Messaging. IT is revolutionizing the way humanitarian organizations provide relief in developing countries. As noted earlier, websites are increasingly used to facilitate communications during emergencies. Thus, it is not surprising that the United Nations' humanitarian affairs office has opened up a website called ReliefWeb. This website for the humanitarian relief community allows aid workers across the world to get up-to-date maps and data on emergencies and disasters around the world—everything from flooding to refugee migration.[112] Individuals affected by natural or other disasters can also use IT to obtain aid. In north Kenya, for example, a refugee with access to a mobile phone sent a text message to United Nations officials noting the lack of food in his camp.[113] Officials responded by increasing food distribution.

Humanitarian aid agencies are using IT in their operations both for emergency communications and to exchange information about supplies and deliveries.[114] Moreover, governments are beginning to see the value of using IT to reach their citizens before disaster strikes. The government of Sri Lanka, for example, has an early-warning system that sends short message service (SMS) messages to every mobile phone in an area at risk of flooding.[115]

Coping with Accidents and Natural Disasters

Governments and nongovernmental organizations are using IT to predict, respond to, and manage accidents at dangerous facilities, as well as natural phenomena such as hurricanes, wildfires, tsunamis, and landslides. Using satellite images, aerial photographs, and on-the-ground inspections, such organizations can locate populations in dangerous or environmentally unstable places and determine how to respond after disaster strikes.[116] The Respond Project, for example, used geographic information system (GIS) data on India and Sri Lanka after the 2004 tsunami to plan improvements in preparedness and prediction.[117] Similarly, a United Kingdom charity, MapAction, responded quickly to several disasters by providing mapping and GIS experts to identify key facilities such as hospitals, food warehouses, and roads. These data were incorporated into digital maps and distributed to relief organizations working in the areas.[118]

Preventing and Dealing with Accidents

Even with comprehensive security controls at dangerous sites such as chemical plants, nuclear power plants, and refineries, use comprehensive security controls, no site is immune to all accidents. When accidents occur at such sites, one goal of emergency responders is to determine if the disaster has created any new threats. In the United States, the National

Atmospheric Release Advisory Center (NARAC) monitors the release of hazardous material into the atmosphere. NARAC provides tools to model and predict the spread of airborne particles from nuclear, radiological, chemical, biological, or natural emissions. NARAC has developed a distributed system that provides three-dimensional modeling of hazards using geographic data and real-time weather information. Using this system, emergency responders can produce initial predictions within minutes and then refine these predictions as new data becomes available from the field. NARAC also provides a tool to map the spread of hazards so emergency workers can notify and protect the affected communities.[119]

Other tools allow researchers to spot and prevent human-made disasters before they happen. Aviation experts working for airlines, for example, regularly comb through large amounts of data collected from computer records of daily flights and pilot incident reports to spot potential hazards, such as areas on the ground or in the air at higher risk of collision. In the United States, the Federal Aviation Administration has even launched a data-mining effort to detect anomalies in data recorded in-flight, including airspeed, pitch angles, engine temperatures, and movements. These efforts ensure that aviation experts can learn lessons not only from past mistakes but also from "near misses" that might reveal some safety flaw.[120] Engineers similarly use IT to study and improve the structural integrity of buildings and bridges. To study the impact of earthquakes on building materials, one university research group at SUNY Buffalo built a complete two-story house on top of an earthquake simulator. The researchers then collected data from 250 sensors spread throughout the house and a series of video cameras. Analyzing these data will enable engineers to construct more stable buildings.[121]

Forecasting Hurricanes

Hurricanes can be incredibly deadly and destructive through a combination of high winds, heavy rain, and large waves. Public officials can mitigate some of the loss of life and destruction from a hurricane if they can accurately predict the hurricane's size and wind speed and when and where the hurricane will make landfall.

Advances in IT have enabled the collection of more precise hurricane data. Much of the information used to track hurricanes in the United States comes from the Doppler radar network established in the 1980s by the National Oceanic and Atmospheric Administration (NOAA). In addition, forecasters use geostationary weather satellites to obtain measurements of hurricane activity and intensity, even in remote ocean areas.[122] To get more detailed information, scientists fly special aircraft into or around the storm to take precise measurements about the structure and intensity of the hurricane. In addition, the scientists release GPS-enabled dropwindsondes, special instruments deployed from the aircraft that drift down on a parachute measuring vertical profiles of pressure, temperature, humidity, and wind as they fall to the earth, and then radio the information back to the scientists.[123] A new technique, recently developed by NOAA has found that computer models can accurately predict a storm's intensity from sound sensors as a hurricane moves in the ocean.[124]

Forecasters use software tools to make precise predictions about flooding based on the latest hurricane data information and information about the coastal terrain.

Once forecasters collect hurricane-related data from radar and satellites, they can use computer models to predict a hurricane's movement. Much of the impact of a hurricane comes from coastal and inland flooding, particularly flooding caused by the storm surge. Forecasters use tools such as the Sea, Lake, and Overland Surges from Hurricanes (SLOSH) model to make precise predictions about flooding based on the latest hurricane data information and information about the coastal terrain. Such models allow public officials to warn and evacuate communities who are most likely to be impacted by a hurricane.

Predicting and Responding to Wildfires

Wildfires ravage thousands of acres of land every year, destroying homes and businesses and killing firefighters, civilians and wildlife. Scientists use IT to help them better predict, manage, and respond to wildfires. They can use dynamic data-driven computer models, for example, to predict a wildfire's progression and help firefighters determine the best response. The mechanics of a wildfire are enormously complex and can be influenced by anything from the weather to the chemistry of the fuel. To accurately predict wildfire behavior, computer models must consider many complex processes and incomplete data sets, a challenge to which today's supercomputers are finally able to respond.[125]

Scientists collect data for wildfire modeling from satellites, aerial photography and surveying, and remote sensors. Remote sensors that can survive low-intensity fires, such as Web-enabled surveillance cameras and fixed autonomous sensors for detecting environmental conditions, offer the potential for real-time updates to firefighters.[126] Such remote sensors can collect measurements such as temperature, wind direction and speed, and moisture levels; send this data to be processed by a computer; and then transmit wildfire prediction maps to the handheld computers of firefighters on the ground.[127] Wildfire prediction information sent to their handheld computers can help firefighters on the ground avoid injury from changing wildfire conditions and allow them to evacuate the most threatened areas.

Geographic information systems (GIS) also enable better data collection and representation. By making it possible to associate data points with specific spatial locations on Earth, GIS make it possible for scientists to more accurately model wildfire behavior and visually represent wildfire predictions on maps such as Google Earth. Firefighters on the ground are also making use of GIS to coordinate and improve their response. Firefighters can use GIS to quickly locate resources such as water or identify locations at risk such as schools.[128] Special technology exists for firefighters to help them locate each other on the scene of the fire and to better monitor firefighters' vital signs and locations. This technology facilitates communications between firefighters and the command center.[129] In addition, firefighters can use handheld computers to record environmental factors, run hydraulic calculators, and predict fire behavior. They can also use handheld computers to consult electronic medical references and emergency translators for access to common medical phrases.[130] Finally, firefighters and ambulance drivers can use GPS to get to locations where they are needed and to locate the nearest hospital.

Detecting Tsunamis in Time to Provide Warnings

Events such as volcanic eruptions, landslides, earthquakes, or even impacts by an asteroid can rapidly displace water to trigger massive ocean waves known as tsunamis. The devastating power of tsunamis was brought to light in 2004 when an earthquake off of the coast of Sumatra generated a tsunami in the Indian Ocean that resulted in the deaths of 230,000 people and displaced millions.[131] The hardest hit countries were Indonesia, Sri Lanka, India, and Thailand.

Tragically, the fact that the Pacific Tsunami Warning Center lacked some of the newer tools to accurately predict the risk of a tsunami hampered early warning efforts for the 2004 tsunami. Using seismological data, the Pacific Tsunami Warning Center initially estimated that the tremors only reached a magnitude of 8.0 rather than the actual magnitude of 9.1. Other computer models could have better gauged the magnitude of the tremors. Within two hours of the quakes, a computer at Harvard University in Massachusetts accurately predicted the higher magnitude of the tremors from the same seismological data; unfortunately, however, that computer was not equipped to send automatic alerts to the Pacific Tsunami Warning Center.[132]

Since 2004, public officials have invested in a more complete early warning system to detect tsunamis and alert coastal areas to a tsunami threat. The result is an international Tsunami Warning System, a network of seismometers, sea-bottom pressure sensors, and tide gauges that continually monitor, collect, and share data on oceanic activity. In addition, coastal areas have invested in better alert systems so public officials can quickly notify communities of a threat.[133]

Predicting Landslides

Landslides pose a serious threat to many urban and

rural areas, causing more than $1 billion dollars in damages and over 25 deaths every year in the United States alone. Although landslides are triggered by other natural disasters, such as earthquakes, volcanoes, wildfires and floods, public safety officials can help reduce losses from such events by identifying landslide hazards and developing mitigation strategies.[134]

IT has played a major role in improving the identification of landslide hazards through the use of advanced modeling and simulation tools and the growth of GIS technology. Landslides are influenced by many complex factors which can be difficult to measure including vegetation type, terrain alignment, soil cohesion and depth to water table. Although scientists are still far from developing complete hazard models, they have improved their techniques for risk assessment. Thus, for example, geologists can use digital elevation models and the related software tools to better understand the terrain and surface topography, which strongly influences the risk of a landslide. In addition, scientists can use GIS-based quantitative and qualitative modeling techniques to more accurately predict landslide susceptibility and generate hazard maps.[135]

Endnotes

1. U.S. Department of Homeland Security, "DHS Begins Collecting 10 Fingerprints from International Visitors at Washington Dulles International Airport," Washington, D.C., December 10, 2007 <www.dhs.gov/xnews/releases/pr_1197300742984.shtm> (accessed July 22, 2008).

2. U.K. Home Office, "Border Control: Frequently Asked Questions," London, n.d. <press.homeoffice.gov.uk/faqs/controlling-our-borders/> (accessed July 22, 2008).

3. APEC Business Mobility Group, APEC Committee on Trade and Investment, Asia-Pacific Economic Cooperation, "Advanced Passenger Information Systems," n.d. <www.businessmobility.org/API/API.html> (accessed May 16, 2008).

4. U.K. Border Agency, "How Does e-Borders work?" n.d. <www.ukba.homeoffice.gov.uk/managingborders/technology/eborders/howebordersworks/> (accessed May 15, 2008).

5. U.K. Home Office, "Iris Recognition Immigration System (IRIS)," London, n.d. <www.ukba.homeoffice.gov.uk/managingborders/technology/iris/> (accessed May 15, 2008).

6. U.K. Home Office, "Biometric Passports," London, n.d. <www.ips.gov.uk/passport/about-biometric-chip.asp> (accessed May 16, 2008).

7. Federal Ministry of the Interior, Federal Republic of Germany, "The e-Passport: Basics," Berlin, Germany, n.d. <www.bmi.bund.de> (accessed May 16, 2008).

8. Australian Customs Service, "SmartGate—Frequently Asked Questions," n.d. <www.customs.gov.au/site/page.cfm?u=5555> (accessed August 8, 2008).

9. U.S. Customs and Border Protection, U.S. Department of Homeland Security, "On Track to Securing America's Borders," May 15, 2006 <www.cbp.gov/xp/cgov/newsroom/highlights/border_sec_news/ontrack.xml> (accessed August 10, 2008).

10. U.S. Customs and Border Protection, U.S. Department of Homeland Security, SBInet Website, n.d. <www.cbp.gov/xp/cgov/border_security/sbi/sbinet_information/> (accessed August 15, 2008).

11. U.S. Department of Homeland Security, "Fact Sheet: Secure Border Initiative," November 2, 2005 <www.dhs.gov/xnews/releases/press_release_0794.shtm> (accessed May 16, 2008).

12. U S. Department of Homeland Security, 2005.

13. Christopher Bolkcom, "Homeland Security: Unmanned Aerial Vehicles and Border Surveillance," Foreign Affairs, Defense, and Trade Division, Congressional Research Service, Library of Congress, Washington, D.C., February 7, 2005 <epic.org/privacy/surveillance/spotlight/0805 /rscb.pdf > (accessed August 8, 2008).

14. Bolkcom, 2005.

15. Bolkcom, 2005.

16. U.S. Customs and Border Patrol, "CSI in Brief," n.d. <www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml> (accessed May 16, 2008).

17. Transportation Security Administration, U.S. Department of Homeland Security, "FAQ: Transportation Worker Identification Credential," n.d. <www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm> (accessed August 8, 2008).

18. Grace Jean, "Building Miniature 'Noses' to Sniff Explosives," *National Defense* 92(647) (October 2007): 16.

19. Jean, "Building Miniature," 2007.

20. Gregory D. Kutz and John W., Cooney, U.S. Government Accountability Office, "Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process," testimony before the House Committee on Government Reform, U.S. Congress, Washington, D.C., November 15, 2007 <www.gao.gov/new.items/d0848t.pdf> (accessed August 8, 2008).

21. Grace Jean, "Beyond X-Ray Machines: Airports Test Alternatives for Checkpoints," *National Defense* 92(647) (October 2007): 30.

22. Jean, "Beyond X-Ray," 2007.

23. Emile Venere and Elizabeth K. Gardner, "Cell Phone Sensors Detect Radiation to Thwart Nuclear Terrorism," *Purdue University* News, January 22, 2008 <news.uns.purdue.edu/x/2008a/080122FischbahNuclear.html> (accessed May 16, 2008).

24. Venere and Gardner, 2008.

25. Erik J. Dahl, "Preventing Terrorist Attacks: Challenging the Conventional Wisdom," *Belfer Center for Science and International Affairs*, May 5, 2008 <belfercenter.ksg.harvard.edu/publication/18249/preventing_terrorist_attacks.html> (accessed May 16, 2008).

26. Heather Havenstein, "Top Secret: CIA Explains its Wikipedia-Like National Security Project," *Computer World*, June 10, 2008 <www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=13&articleId=9095638> (accessed August 8, 2008).

27. David Gardner, "Enterprise 2.0: CIA's Secret Intellipedia Has Universal Relevance," *Information Week*, June 10, 2008 <www.informationweek.com/news/business_intelligence/mining/showArticle.jhtml?articleID=208403131> (accessed August 12, 2008).

28. Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview," Congressional Research Service, Library of Congress, Washington, D.C., updated January 18, 2007 <www.fas.org/sgp/crs/intel/RL31798.pdf> (accessed August 8, 2008).

29. Financial Crimes Enforcement Network, U.S. Department of the Treasury, "Support of Law Enforcement," n.d. <www.fincen.gov/law_enforcement/les/> (accessed August 8, 2008).

30. Financial Crimes Enforcement Network, n.d.

31. Kristin Archick et al., "European Approaches to Homeland Security and Counterterrorism," Congressional Research Service, Library of Congress, Washington, D.C., July 24, 2006 <www.fas.org/sgp/crs/homesec/RL33573.pdf> (accessed August 8, 2008).

32. Australian Transactions Reports and Analysis Centre, "Research and Analysis," n.d. <www.austrac.gov.au/research_and_analysis.html> (accessed May 19, 2008).

33. Australian Government Department of the Prime Minister and Cabinet, "The National Security Science and Technology Branch of the Office of National Security," updated March 17, 2008 <www.dpmc.gov.au/nsst/docs/research_support_grant_recipients_2008.pdf> (accessed August 8, 2008).

34. Eric Lichtblau and James Risen, "Bank Data Is Sifted by U.S. in Secret to Block Terror," *New York Times*, June 23, 2006 <www.nytimes.com/2006/06/23/washington/23intel.html> (accessed August 8, 2008).

35. Lichtblau and Risen, 2006.

36. Archick et al., 2006.

37. Rob Hendin, "FBI's New Data Warehouse A Powerhouse," CBS News, August 30, 2006 <www.cbsnews.com/stories/2006/08/30/terror/main1949643.shtml> (accessed August 8, 2008).

38. Hendin, 2006.

39. U.S. Department of State, "Facts About Human Trafficking," December 7, 2005 <www.state.gov/g/tip/rls/fs/2005/60840.htm> (accessed May 19, 2008).

40. U.S. Agency for International Development, "MTV EXIT: Youth-Focused Campaign to End Exploitation and Trafficking," n.d. <www.usaid.gov/our_work/global_partnerships/gda/resources/ane_mtv_exit.pdf> (accessed August 8, 2008).

41. Asia Foundation, "Utilizing Information Technology to Address Human Trafficking," n.d. <www.asiafoundation.com/pdf/trafficking-IT.pdf> (accessed May 19, 2008).

42. Asia Foundation, n.d.

43. United Nations Educational, Scientific and Cultural Organization, "GIS-Linked Social Sentinel Surveillance Project," n.d. <www.unescobkk.org/index.php?id=1820> (accessed May 15, 2008).

44. Asia Foundation, n.d.

45. Frank Laczko, "Data and Research on Human Trafficking," *International Migration*, 43 no. 1 (2005): 5-16.

46. Barbara Depompa, "Alexandria Police Go Wireless Remote," *FCW.com* January 31, 1997 <www.fcw.com/print/3_5/news/60642-1.html> (accessed August 8, 2008).

47. Hugh Downing, "The Emergence of Global Positioning Satellite (GPS) Systems in Correctional Applications," *Corrections Today*, July 2005 <www.aca.org/fileupload/177/prasannak/downing.pdf> (accessed August 8, 2008).

48. Downing, July 2005.

49. Joe Russo, "Emerging Technologies for Community Corrections," Corrections Today, October 2006 <www.aca.org/fileupload/177/prasannak/russo.pdf> (accessed May 19, 2008).

50. Robert D. Atkinson, *Network Government for the Digital Age* (Washington, D.C.: Progressive Policy Institute, 2003) <www.ppionline.org/documents/NetGov_0503.pdf> (accessed August 8, 2008).

51. Joe Russo, "Emerging Technologies for Community Corrections," *Corrections Today*, October 2006 <www.aca.org/fileupload/177/prasannak/russo.pdf> (accessed May 19, 2008).

52. Ontario (Canada) Ministry of Transportation, "Ignition Interlock," n.d. <www.mto.gov.on.ca/english/safety/impaired/interlock> (accessed August 8, 2008).

53. Turner-Fairbank Highway Research Center, Federal Highway Administration, U.S. Department of Transportation, "Safety Evaluation of Red-Light Cameras-Executive Summary," 2005 <www.tfhrc.gov/safety/pubs/05049/05049.pdf> (accessed May 15, 2008).

54. Richard A. Retting, Susan A. Ferguson, and A. Shalom Hakkert, "Effects of Red Light Cameras on Violations and Crashes: A Review of the International Literature," *Traffic Injury Prevention* 4 (March 2003): 17 <pdfserve.informaworld.com/Pdf/AddCoversheet?xml=/mnt/pdfserve/pdfserve/829801--713712743.xml> (accessed August 15, 2008).

55. Elizabeth Alicandri and Davey L. Warren, "Managing Speed," *Public Roads*, January 2003 <www.tfhrc.gov/pubrds/03jan/10.htm> (accessed August 8, 2008).

56. Alicandri and Warren, 2003.

57. Keri Funderburg "Internet Watch," *Public Roads*, January 2003 <www.tfhrc.gov/pubrds/03jan/iwatch.htm> (accessed August 8, 2008).

58. Richard Abshire and Tanya Eiserer, "Surveillance Cameras in Dallas Area Work to Counter Crime,"Dallas Morning News, March 21, 2008 <www.dallasnews.com/sharedcontent/dws/news/localnews/crime/stories/032208dnmetcameras.392cac9.html> (accessed August 8, 2008).

59. Richard Willing, "Airport Anti-Terror Systems Flub Tests," *USA Today*, September 2, 2003 <www.usatoday.com/travel/news/2003/09/02-air-secur.htm> (accessed August 8, 2008).

60. Willing, 2003.

61. Kevin W. Bowyer, "Face Recognition Technology: Security Versus Privacy," *IEEE Technology and Society Magazine* 23(1) (Spring 2004): 9 <ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/44/28491/01273467.pdf?temp=x> (accessed August 8, 2008).

62. Mark Landler, "Where Little Is Left Outside the Camera's Eye," *New York Times*, July 8, 2007 <www.nytimes.com/2007/07/08/weekinreview/08landler.html> (accessed August 8, 2008).

63. Bowyer, 2004.

64. "Image of Bombers' Deadly Journey," BBC News, July 17, 2005 <news.bbc.co.uk/2/hi/uk_news/politics/4689739.stm> (accessed August 8, 2008).

65. Bowyer, 2004.

66. Steve Conner, "Britain Will Be First Country to Monitor Every Car Journey," *The Independent*, December 22, 2005 <www.independent.co.uk/news/uk/home-news/britain-will-be-first-country-to-monitor-every-car-journey-520398.html> (accessed August 8, 2008).

67. Seattle Police Department, "License Plate Recognition Camera," n.d. <www.seattle.gov/police/programs/technology/license_plate_reader.htm> (accessed August 8, 2008).

68. Jim McKay, "Police Tout License Plate Recognition Systems as the Next Big Thing," *GovTech.com*, May 12, 2008 <www.govtech.com/gt/273037> (accessed August 8, 2008).

69. D. Weisburd et al., "The Growth of COMPStat in American Policing," Police Foundation, Washington, D.C., 2004 <www.policefoundation.org/pdf/growthofcompstat.pdf> (accessed August 8, 2008).

70. Philadelphia Police Department, "Philadelphia Police Department: COMPStat Process," 2008 <www.ppdonline.org/hq_compstat.php> (accessed August 8, 2008).

71. Ned Levine et al., "Crime Mapping and the *CrimeStat* Program," *Geographical Analysis* 38(1) (2006): 41.

72. Levine et al., 2006.

73. Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, "Firearms and Crime Statistics," updated March 1, 2007 <www.ojp.usdoj.gov/bjs/guns.htm> (accessed August 8, 2008).

74. Fernicia Patrick and Tod W. Burke, "Gunshot Sensor Technology: Can You Hear Me Now?" *Police and Security News* 23(3) (May-June 2007): 1 <www.shotspotter.com/news/articles/2007/7%20-%20July/Police%20&%20Security%20News_Gun%20Shot%20Sensors_May-June%202007.pdf> (accessed August 15, 2008).

75. Paul Johnson and Robin Williams "Internationalising New Technologies of Crime Control: Forensic DNA Databasing and Datasharing in the European Union," *Policing and Society* 17(2) (2007): 103.

76. Helen Wallace, "The U.K. National DNA Database: Balancing Crime Detection, Human Rights, and Privacy," *European Molecular Biology Organization* (EMBO) Reports 7 (2006): S26 <www.nature.com/embor/journal/v7/n1s/full/7400727.html> (accessed August 15, 2008).

77. Kristin Archick et al., *European Approaches to Homeland Security and Counterterrorism* (Washington, D.C.: Congressional Research Service, Library of Congress, July 24, 2006). <www.fas.org/sgp/crs/homesec/RL33573.pdf> (accessed August 15, 2008).

78. Innocence Project, "Facts on Post-Conviction DNA Exonerations," n.d. <www.innocenceproject.org/Content/351.php> (accessed August 8, 2008).

79. U.S. President's DNA Initiative, "Solving Cold Cases," n.d. <www.dna.gov/uses/solving-crimes/cold_cases/> (accessed August 10, 2008).

80. U.S. President's DNA Initiative, "DNA Captures Night Stalker," n.d. <www.dna.gov/case_studies/night_stalker> (accessed May 22, 2008).

81. National Registration Department, Ministry of Home Affairs, Malaysia, "MyKad: The Government Multipurpose Card," n.d. <www.jpn.gov.my/kppk1/Index2.htm> (accessed August 8, 2008).

82. National Registration Department, Malaysia, n.d.

83. Hong Kong, "HK Smart Identity Card: Frequently Asked Questions," revised March 31, 2008 <www.smartid.gov.hk/en/faq/index.html> (accessed August 10, 2008).

84. Directorate of the Police and Civil Guard, Ministry of the Interior, Government of Spain,"Listado de Preguntas Frecuentes Sobre DNI Electrónico," n.d. <www.dnielectronico.es/Preguntas_Frecuentes/expedicion/index.html> (accessed August 10, 2008).

85. Carl Lundberg, "Assessment of Man-Portable Robots for Law Enforcement Agencies," doctoral thesis, KTH School of Computer Science and Communication, Stockholm, Sweden, 2007 <www.diva-portal.org/kth/theses/abstract.xsql?dbid=4540> (accessed August 10, 2008).

86. Battelle, "Law Enforcement Robot Technology Assessment, Final Report," prepared for the Counter Terrorism Technology Support Office (CTTSO), National Institute of Justice, U.S. Department of Justice, Washington, D.C., April 2000 <www.nlectc.org/jpsg/robotassessment/robotassessment.html> (accessed August 10, 2008).

87. Raymond E. Foster, "Crime Scene Investigation," *Government Technology*, March 2, 2005 <www.govtech.com/gt/articles/93225> (accessed August 10, 2008).

88. Portland Police Department, City of Portland, Oregon, "CrimeMapper," n.d. <www.portlandonline.com/police/index.cfm?c=29830> (accessed April 2, 2008).

89. Sean Scully, "Letting Victims Track Their Tormentors," *Time*, May 2008 <www.time.com/time/nation/article/0,8599,1807730,00.html> (accessed July 31, 2008).

90. Scot Wortley and Julian Tanner, "Data, Denials, and Confusion: The Racial Profiling Debate in Toronto," *Canadian Journal of Criminology and Criminal Justice*, July 1, 2003 <www.ncjrs.gov/App/publications/Abstract.aspx?id=203433> (accessed August 15, 2008).

91. The Justice Project, *Electronic Recording of Custodial Interrogations* (Washington, D.C.: The Justice Project) <www.thejusticeproject.org/national/solution/electronic-recording-of-custodial-interrogations/> (accessed August 10, 2008).

92. The Justice Project, n.d.

93. Hector Castro, "Police Cars Get Digital Cameras," *Seattle Post Intelligencer*, December 18, 2004 <seattlepi.nwsource.com/local/204326_cameras18.html> (accessed August 10,

2008).

94. "Taser Video Again Questions Police Behavior," MSNBC New Service, November 18, 2006 <www.msnbc.msn.com/id/15765622/print/1/displaymode/1098/> (accessed August 10, 2008).

95. B. S. Manoj and Alexandra Hubenko Baker, "Communication Challenges in Emergency Response," *Communications of the ACM* 50 (3) (2007): 51 <portal.acm.org/citation.cfm?id=1226736.1226765&coll=GUIDE&dl=GUIDE&CFID=29969974&CFTOKEN=38142168> (accessed August 15, 2008).

96. Jon M. Peha, "Broadband and IP for Public Safety," presentation at the ITIF Forum: IP and Broadband Technology—Working for Public Safety, sponsored by the Information Technology and Innovation Foundation, Washington, D.C., July 23, 2007 <www.itif.org/files/PehaPresentation.pdf> (accessed August 10, 2008).

97. National Crime Information Center, Criminal Justice Information Services Division, Federal Bureau of Investigation, U.S. Department of Justice, "National Crime Information Center," 2008 <www.fbi.gov/hq/cjisd/ncic_brochure.htm> (accessed August 10, 2008).

98. Northrop Grumman Corp., "Northrop Grumman, NextWave Wireless, Successfully Test Public Safety Network Solution and Enable First Real-Time Remote Crime Scene Investigation in the U.K.," press release, London, April 23, 2008 <www.irconnect.com/noc/press/pages/news_releases.html?d=140770> (accessed August 10, 2008).

99. BelAir Networks, "Beaverton, Oregon Builds Interoperable Public Safety Wireless Network," 2007 <www.belairnetworks.com/resources/pdfs/Beaverton_PubSaf_CS_BDMD0001-A01.pdf> (accessed August 10, 2008).

100. Federal Communications Commission, "In the Matters of Review," 2007.

101. Public Safety and Homeland Security Bureau, Federal Communications Commission, "Emergency Alert System," n.d. <www.fcc.gov/pshs/services/eas/index.html> (accessed August 10, 2008).

102. Office of Justice Programs, U.S. Department of Justice, "AMBER Alert" n.d. <www.amberalert.gov> (accessed March 28, 2008).

103. The West Virginia High Technology Consortium, "What Is AmberView?" n.d. <www.amberview.org> (accessed March 28, 2008)

104. Federal Emergency Management Agency, U.S. Department of Homeland Security, "Integrated Public Alert and Warning System (IPAWS)," Washington, D.C., updated November 11, 2007 <www.fema.gov/emergency/ipaws/> (accessed August 10, 2008).

105. Sascha Meinrath, "Disaster Response: The Good, the Bad, and the Ugly," *Government Technology*, December 18, 2006 <www.govtech.com/gt/articles/102914> (accessed July 31, 2008).

106. National Emergency Number Association, "Wireless E-911 Saves," January 22, 2006, <www.nena.org/pages/Content.asp?CID=70&CTID=10> (accessed July 31, 2008).

107. "Katrina PeopleFinder Project," Wikipedia, updated December 12, 2005 <katrinahelp.info/wiki/index.php/Katrina_PeopleFinder_Project> (accessed May 27, 2008).

108. Pamela LiCalzi O'Connell, "Internet Matchmaking: Those Offering Help and Those Needing It," *New York Times*, November 14, 2005 <www.nytimes.com/2005/11/14/giving/14oconnell.html> (accessed August 10, 2008).

109. "Main Page: Katrina Help Info," Wikipedia, updated December 14, 2005 <katrinahelp.info/wiki/index.php/Main_Page> (accessed May 27, 2008).

110. Robert Scoble, "Twittering the Earthquake in China," n.d. <www.scobleizer.com/2008/05/12/quake-in-china/> (accessed August 10, 2008).

111. Kevin Poulsen, "Firsthand Reports from California Wildfires Pour Through Twitter," Wired Blog Network, October 23, 2007 <blog.wired.com/27bstroke6/2007/10/firsthand-repor.html> (accessed August 10, 2008).

112. "Dealing with Disasters: Flood, Famine, and Mobile Phones," *The Economist*, July 28, 2007: 65.

113. "Dealing with Disasters," 2007.

114. "Dealing with Disasters," 2007.

115. "Dealing with Disasters," 2007.

116. Randall B. Kemp and Sanjeev Khagram, "When the Land Tells a Story: Using Geographic Information Systems (GIS) for Landscape Monitoring and Humanitarian Relief," *Innovations* 1(2) (Spring 2006): 68.<www.mitpressjournals.org/doi/abs/10.1162/itgg.2006.1.2.68> (accessed August 15, 2008).

117. Kempt and Khagram, 2006.

118. Kempt and Khagram, 2006.

119. John S. Nasstrom et al., "The National Atmospheric Release Advisory Center (NARAC) Modeling and Decision Support System for Radiological and Nuclear Emergency Preparedness and Response," *International Journal of Risk Assessment and Management, Special Issue: Nuclear and Radiological Emergency Preparedness—The Role of Monitoring and Modeling in an Emergency Situation*, April 25, 2005 <narac.llnl.gov/uploads/Nasstrom_et_al_2006_IJRAM_NARAC_211678_hdbde.pdf> (accessed August 10, 2008).

120. Del Quintin Wilber, "Avoiding Plane Crashes by Crunching Numbers," *Washington Post*, January 13, 2008: A7 <www.washingtonpost.com/wp-dyn/content/article/2008/01/12/AR2008011202407.html> (accessed August 10, 2008).

121. Greta Lorge, "Rock the House," *Wired* 14(11) (November 2006) <www.wired.com/wired/archive/14.11/start.html?pg=9> (accessed August 10, 2008).

122. Nan D. Walker et al., "Hurricane Prediction: A Century of Advances," *Oceanography* 19 (2) (June 2006): 24 <www.tos.org/oceanography/issues/issue_archive/issue_pdfs/19_2/19.2_walker_et_al.pdf> (accessed August 10, 2008).

123. National Oceanic and Atmospheric Administration, U.S. Department of Commerce, "NOAA's 'Hurricane Hunter' Aircraft," updated March 23, 2003 <www.publicaffairs.noaa.gov/grounders/hurricanehunters.html> (accessed August 10, 2008).

124. Arlene Weintraub, "The Ear of the Hurricane," *BusinessWeek*, April 28, 2008; posted April 17, 2008 <www.businessweek.com/magazine/content/08_17/c4081scitech888608.htm> (accessed August 10, 2008).

125. Stephanie vL Henkel, "Fire on the Mountain! Run, Boys, Run!" *Sensors Online* (September 2004) <archives.sensorsmag.com/articles/0904/10/main.shtml> (accessed August 8, 2008).

126. Jan Mandel et al. ,"A Dynamic Data Driven Wildland Fire Model," Yong Shi et al. (eds), *Lecture Notes in Computer Science 4487, Part I; International Conference on Computational Science 2007* (Berlin-Heidelberg: Springer-Verlag, 2007): 1042 <www-math.cudenver.edu/~jmandel/fires/papers/iccs07-paper.pdf> (accessed August 15, 2008).

127. Henkel, 2004.

128. Russ Johnson and Ron Bisio, "Mobile GIS Shrinks Information Gap for Wildfire Decision Makers," *ArcUserOnline*, October-December 2004 <www.esri.com/news/arcuser/1104/wildfire_gps1of2.html> (accessed August 10, 2008).

129. Charles Werner, "New Technology for Firefighter Accountability and Safety," *Firehouse.com*, June 18, 2007 <cms.firehouse.com/web/online/Technology-and-Communications/New-Technology-for-Firefighter-Accountability-and-Safety/13$55131> (accessed August 10, 2008).

130. "PDA Resources on the Web," *Firehouse.com*, updated September 26, 2007 <www.firehouse.com/tech/pda.html> (accessed August 10, 2008).

131. U.S. Geological Survey, U.S. Department of the Interior, "Most Destructive Known Earthquakes on Record in the World," updated July 16, 2008 <earthquake.usgs.gov/regional/world/most_destructive.php> (accessed August 10, 2008).

132. Richard A. Kerr, "Failure to Gauge the Quake Crippled the Warning Effort," *Science* 307(5707) (2005): 201 <www.sciencemag.org/cgi/content/summary/307/5707/201?ck=nck> (accessed August 10, 2008).

133. Dennis Normile, "Tsunami Warning System Shows Agility—And Gaps in Indian Ocean Network," Science, 317 (5845) (2007): 1661 <www.sciencemag.org/cgi/content/summary/317/5845/1661?etoc=> (accessed August 10, 2008).

134. U.S. Geological Survey, U.S. Department of the Interior, "Landslides Hazards Program," updated June 11, 2008 <landslides.usgs.gov> (accessed July 31, 2008).

135. Alberto Carrara and Richard J. Pike, "GIS Technology and Models for Assessing Landslide Hazard and Risk," *Geomorphology* 94(3) (2008): 257.

About the Information Technology and Innovation Foundation

ITIF is a non-profit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington DC and in the states. Recognizing the vital role of technology in ensuring American prosperity, ITIF focuses on innovation, productivity, and digital economy issues.

Technological innovation, particularly in information technology, is at the heart of America's growing economic prosperity. Crafting effective policies that boost innovation and encourage the widespread "digitization" of the economy is critical to ensuring robust economic growth and a higher standard of living. However, as in any new and changing situation, policymakers have varied awareness of what is needed and what will work. In some cases legislators have responded to new and complex technology policy issues with solutions more suited for the old economy. And as the innovation economy has become increasingly important, opposition to it from special interests has grown. Finally, the excitement that the press, pundits and decision makers showed toward the information technology (IT) revolution in the 1990s has all too often been replaced with an attitude of "IT doesn't matter." It is time to set the record straight—IT is still the key driver of productivity and innovation.

As a result, the mission of the Information Technology and Innovation Foundation is to help policymakers at the federal and state levels to better understand the nature of the new innovation economy and the types of public policies needed to drive innovation, productivity and broad-based prosperity for all Americans.

ITIF publishes policy reports, holds forums and policy debates, advises elected officials and their staff, and is an active resource for the media. It develops new and creative policy proposals to advance innovation, analyzes existing policy issues through the lens of advancing innovation and productivity, and opposes policies that hinder digital transformation and innovation.

To find out more about the Information Technology and Innovation Foundation, please contact us at 1250 I Street, NW, Suite 200, Washington, DC 20005.

E-mail: mail@itif.org. Phone: (202) 449-1351.
Web: www.innovationpolicy.org