Law Enforcement Executive

FORUM

Terrorism - Special Edition

March 2002

Illinois Law Enforcement Executive Forum Special Edition
Illinois Law Enforcement Training and Standards Board
in cooperation with Western Illinois University
Macomb, IL 61455

Editorial Production
Curriculum Publications Clearinghouse, Macomb, Illinois

Production Assistant
Linda Brines

The *Illinois Law Enforcement Executive Forum* is published semiannually by the Illinois Law Enforcement Training and Standards Board's Executive Institute. The journal is sponsored by Western Illinois University in Macomb, Illinois.

Institutional Subscription: $40
Personal Subscription: $25

Disclaimer

Reasonable effort has been made to make the articles herein accurate and consistent. Please address questions about individual articles to their respective author(s).

Table of Contents

Homeland Security

Anti-Terrorism Technique and Technology

Terrorism and the Media

Materials/publications are available through the Illinois Law Enforcement Executive Institute.

Editorial

The focus of this edition of the *Illinois Law Enforcement Executive Forum* is terrorism. While intense international and domestic efforts to combat terrorism take priority, local law enforcement is waiting in the wings. Major city police agencies have always been aware, at some level, of the potential of direct threats to their jurisdictions by terrorists. While New York City, Chicago, Los Angeles, and other jurisdictions of similar populations are redoubling their efforts to protect themselves against terrorists, the role and required response of smaller law enforcement agencies is less clear.

One thing we do know is that all of law enforcement must prepare for, and participate in, efforts to gather intelligence information on potential terrorist activities, and must have a coordinated plan of response. This is a new era for law enforcement—a new priority. Knowledge is the key to preparedness.

The collection of articles in this edition represent a broad spectrum of history, perspective, and thought on the topic of terrorism. This collection of articles is designed as a primer for the considerable discussion, planning, and policy development that is ongoing, at the international, national, and local levels, in response to the terrorist attack against the United States on September 11, 2001.

To a large extent, the considerable amount of Federal funding to combat terrorism currently being proposed by President Bush will influence and direct the actions and response of law enforcement and emergency services at the local level. While awaiting direction, we must forge ahead by gathering as much topical knowledge and information as possible, so that we are adequately informed for response. It is our hope that this edition of the *Forum* contributes to this process of learning.

Thomas J. Jurkanin, PhD
Executive Director
Illinois Law Enforcement Training and Standards Board

Terrorism and Countering the Threat

Jeremy R. Spindlove

Policing in the new millennium will present challenges for American police departments not previously experienced. *Globalization*, a term we hear frequently now must include terrorism within the borders of the United States. Until September 11, 2001, the realities for policing terror incidents of any magnitude and especially international terror attacks was something conducted elsewhere, but not on U.S. soil. The only exceptions were the World Trade Center bombing in 1993 and the homegrown terror attack conducted by Timothy McVeigh in Oklahoma City in May 1995. The unimaginable events of September 11 and the inability of intelligence organizations to gather, fully appreciate, detect, or disseminate any intelligence related to this attack are dumbfounding. Combined with the devastating lapses, perceived or otherwise, by the FAA only added to the exposure of the United States. We now enter what I refer to as the era of "tombstone technology," a status at which the body count has become so horrific that actions have to be taken to correct, reorganize, and reestablish policy, procedures, and programs to protect all aspects of commercial aviation. The catastrophic events of the Pan Am Flight 103 bombing over Lockerbie, Scotland in 1998 was a wake-up call for the world of aviation, but the United States continued to doze . . . protected by two vast oceans. A great many nations initiated changes that were needed to protect aviation; however, many will now have to agree with me that was not the consistent case in United States domestic aviation.

We have been told that the events of September 11, 2001 have changed our lives forever, which may well be the case and will no doubt be established as a historical date and fact at some point in the future. Law enforcement is concerned with the present and must try to understand and react to a changing role for both law enforcement and the intelligence communities of the world. Martyrdom has been and will continue to be one of the signatures of the Islamic terrorists. Hamza akl Hamieh, one of the most fearless fighters for Islam and a military commander for Amal, made the following statement soon after the bombing of the U.S. Marine Corps barracks in Beirut in 1983: " None of us are afraid. God is with us and gives us strength. We are making a race like horses to see who goes to God first. I want to die before my friends. They want to die before me. We want to see our God. We welcome the bombs of Reagan."[1]

Terrorism is founded on fear. Sun Tzu, the great Chinese warrior/philosopher said, "Kill one; frighten a thousand." When fear is absent or well controlled, terrorism will fail. Unfortunately what we have been witnessing since the September 11 attacks is clearly a win/win scenario for the terrorist. Sprinkle some anthrax in envelopes; send some mail to well placed media moguls and politicians, and North America becomes seized by near panic. This would appear to be out of proportion to the actual threat. Every unusual letter or package has Americans reaching for the phone to call emergency services. Stretching our emergency services to the limit no doubt plays into the terrorists' hands. To address terrorism in its worldwide capacity, however, it is crucial to learn some defining points about terrorism and to have some sense of the problem facing the western world in the 21st century. The following statements were made by Sheikh Hassan al Banna, founder of the Muslim Brotherhood terror organization: "It is the nature of Islam to dominate, not to be

dominated, to impose its law on all nations, and to extend its power to the entire planet. The dagger, the poison, the revolver . . . These are weapons of Islam against its enemies." These statements were made two decades before the attack on the World Trade Center in New York on September 11. The growth of Islamic Fundamentalism was first noticed in the early part of the 1990s, and we should not lose sight of the fact that one-fifth of the world's population are followers of the Islamic faith. China has three times as many Muslims as Saudi Arabia, and 32 countries have Muslim majorities of 85% or higher. Of the total Muslim population, approximately 10% is Shi'a, which have constituted the most deadly religious terror groups.[2] The Shi'a sect represents almost 90% of the population of Iran and 60% of the population in Iraq with similarly large percentages in other mid-eastern states such as Bahrain, Lebanon, and Qatar. Twenty-one years ago, in 1979, Iran's now deceased Ayatollah Khomeini stated, "Islam is the religion of militant individuals who are committed to truth and justice; it is the religion of those who desire freedom and independence. It is the school of those who struggle against imperialism . . . . Weapons in our hands are used to realize divine and Islamic aspirations."[3] It is clear that many of his followers still adhere fanatically to his declarations by their actions. In truth, what we have been witnessing is terror organizations hijacking a basically gentle religion for a specific cause or course of action. Clearly Islam is not a religion of hate, fear, or violence; and one needs only to read sections of the Koran to appreciate and understand that point of view.

A historical perspective may help to define the term *terrorism* in regard to a specific time and particular locale. First, we must accept that terrorism, in one form or another, has been around throughout the history of man and society; it did not suddenly appear as a whole new concept in the 20th and 21st centuries. The statement, "One man's terrorist is another man's patriot," must always be related to the time and location in which it is occurring. We have seen many examples of yesterday's terrorist becoming today's national leader in the historical, political, and economic context of change in which terrorism must be operationally defined. History has used the ideologies of both the left and right in the application of what has been loosely termed "terrorism." The understanding of ideological pressures over time allows us to deal with the reasons put forth for terrorist acts in both the last century and the dawn of this one. The ideological commitment of the perpetrators of terrorism can be seen more clearly in this context. The bombing of Pan Am over Lockerbie, Scotland; Japanese tourists massacred in Egypt; the Sarin gas attack on a Tokyo subway; the Oklahoma City bombing; the World Trade Center in New York City; and the Pentagon in Washington, DC all are seen in a common threat when viewed from the perspective of the terrorist. This in no way justifies such acts, but it does lead us to a better (albeit fuzzy) understanding of the political, religious, and ideological fanaticism that creates a terrorist and leads to acts of terror.

In the case of the present threat from Osama bin Laden, it is important to appreciate that his organizational structure is complex by design. During the 1980s, resistance fighters in Afghanistan developed a worldwide recruitment and support network with the aid of the U.S., Saudi Arabia, and other states. After the 1989 Soviet withdrawal, this network, which equipped, trained, and funded thousands of Muslim fighters, came under the control of Osama bin Laden. Al Qaeda ("The Base") is a conglomerate of groups spread throughout the world operating as a network. It has a global reach, with a presence in Algeria, Egypt, Morocco, Turkey, Jordan, Tajikistan, Uzbekistan, Syria, Xinjiang in China, Pakistan, Bangladesh, Malaysia, Myanmar, Indonesia,

Mindanao in the Philippines, Lebanon, Iraq, Saudi Arabia, Kuwait, Bahrain, Yemen, Libya, Tunisia, Bosnia, Kosovo, Chechnya, Dagestan, Kashmir, Sudan, Somalia, Kenya, Tanzania, Azerbaijan, Eritrea, Uganda, Ethiopia, and in the West Bank and Gaza. Since its creation in 1988, Osama bin Laden has controlled al Qaeda. As such, he is both the backbone and the principal driving force behind the network:

Vertically, al Qaeda is organized with bin Laden, the emir-general, at the top, followed by other al Qaeda leaders and leaders of the constituent groups. Horizontally, it is integrated with 24 constituent groups. The vertical integration is formal; the horizontal integration, informal. Immediately below bin Laden is the Shura Majlis, a consultative council. Four committees report to the Shura Majlis: (1) military, (2) religious-legal, (3) finance, and (4) media. Handpicked members of these committees—especially the military committee—conduct special assignments for bin Laden and his operational commanders. To preserve operational effectiveness at all levels, compartmentalization and secrecy are paramount. While the organization has evolved considerably since the United States embassy bombings in Africa in 1999, the basic structure of the consultative council and the four committees remains intact. Bin Laden's intention to expand his operations has been curbed by the post-bombing security environment, and both bin Laden and al Qaeda have been forced to become increasingly clandestine.[4]

Definition

It is important to have an understanding of how difficult it has been to define the word *terrorism*. There are divergent views on what actually constitutes terrorism. Reaching a general consensus on a definition has generated many debates within the social sciences. No single definition completely satisfies the broad spectrum of terrorism. As we see throughout the world whether it be here in the west, the Middle East, sub-Saharan Africa, or the Far East, terrorism is a special type of violence. The worldwide threat is ever present and is a tactic used in conflict, peace, and war. Combating terrorism requires a continuous state of awareness. In fact, it becomes a necessary practice rather than a type of military operation. Categorizing someone as a terrorist does not preclude that person from being categorized as a freedom fighter, guerrilla, ideologue, revolutionary, or even a madman. A police officer who plays football on a weekend can be called a football player, but he has not stopped being a police officer. In fact, members of paramilitary terror groups such as the Provisional IRA, the Real IRA, members of the Basque terror group ETA, and members of Palestinian terror organizations can be termed "freedom fighters" by their sub-group in a political system. To others—governments, the media, and the public at large—the system can brand them as terrorists. But without some reference to established definitional parameters, such labels are purely a matter of value judgment. If the person making the judgment does not agree with the objectives of the group using such methods to gain some goal, they may well describe the group as "terrorist." Invariably, the groups' response will be that it is a "workers' army" or an "army of liberation," but never do they acknowledge the label "terrorists." In addition to the broad definition, the following are examples of the diverse definitions used to describe terrorism:

- Simple – Violence or threatened violence intended to produce fear or change.
- Legal – Criminal violence, violation of legal codes and punishable by the state.

- Analytical – Specific political and social factors behind individual terrorist acts.
- State-Sponsored – Terrorist groups used to attack Western interests.
- State – Power of the government, used to terrorize its people into submission

Even the U.S. Government cannot yet agree on a single definition for terrorism, but these are some of the more commonly used definitions:

- Terrorism is the use or threatened use of force designed to bring about political change. – Brian Jenkins
- Terrorism constitutes the illegitimate use of force to achieve a political objective when innocent people are targeted. – Walter Laqueur
- Terrorism is the premeditated, deliberate, systematic murder, mayhem, and threatening of the innocent to create fear and intimidation in order to gain a political or tactical advantage, usually to influence an audience. – James M. Poland
- Terrorism is the unlawful use or threat of violence against persons or property to further political or social objectives. It is usually intended to intimidate or coerce a government, individual, or group, or to modify their behavior or politics. – U.S. Vice President's Task Force 1986
- Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. – Federal Bureau of Investigation
- Terrorism is the calculated use of violence or the threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. – U.S. Department of Defense

In the U.S., it is the responsibility of the FBI to investigate terrorist groups and acts of terrorism aimed at U.S. citizens both at home and overseas. The FBI has developed a most useful construct of what is to be considered terrorism in the United States. This issue concerns foreign-power-sponsored or foreign-power-coordinated activities that . . .

1. Involve violent acts, dangerous to human life, that are a violation of the criminal laws of the United States or of any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state.

2. Appear to be intended to . . .

   - Intimidate or coerce a civilian population.
   - Influence the policy of a government by intimidation or coercion.
   - Affect the conduct of a government by assassination or kidnapping.

3. Occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

The FBI received its responsibilities through a series of presidential decisions and legislative acts. The most important of these include the following:

- In April 1982, President Ronald Reagan signed a National Security Decision Directive giving the FBI the responsibility for investigating terrorism within the United States.

- The Comprehensive Crime Control Act of 1984 addressed the FBI's role in response to hostage taking.

- The Omnibus Diplomatic security and administration Act of 1986 expanded the FBI's jurisdiction to include investigating acts of terrorism directed against Americans overseas.

- In 1995, President Clinton signed the Presidential Decision Directive 39, entitled *U.S. Policy on Counter-Terrorism*, that further articulated and defined the roles of members of the U.S. Counter-Terrorism Community, including the FBI.

Terrorism, as defined by the U.S. Department of State, is normally considered to be calculated . . . which simply means that terrorists generally know what they are doing. Their selection of a target is planned and rational. They know the effect they seek. Terrorist violence is neither spontaneous nor random in nature. Terrorism is intended to produce fear in someone other than the victim. In other words, terrorism is a psychological act conducted for its impact on a wider audience. In a sense, terrorists' goals are always political, as extremists driven by religious or ideological beliefs usually seek political power to compel society to conform to their views. The objectives of terrorism distinguish it from other violent acts aimed at personal gain, such as criminal violence. The definition, however, does permit including violence by organized crime when it seeks to influence government policy. The essence of terrorism is the intent to induce fear in someone other than the victims to make a government or other audience change its political behavior.

Terrorism that is motivated by religious imperatives is growing quickly, increasing the number of killings and reducing the restraints on mass indiscriminate murder. So great is this change, according to Bruce Hoffman, that we may have to revise our notions of the stereotypical terrorist organization. "Holy Terror" and the purely so-called "secular terror" have radically different value systems, mechanisms for justifying their acts, and concepts of morality. For the religious terrorist, violence is a divine duty. Whereas secular terrorists generally regard indiscriminate violence as immoral and counter productive, religious terrorists view such violence as both morally justified and necessary. Also, whereas secular terrorists attempt to appeal to a constituency composed of sympathizers and the aggrieved people they claim to speak for, religious terrorists act for no audience but themselves. This absence of constituency, combined with an extreme sense of alienation, means that such terrorists can justify almost limitless violence against virtually any target that is not a member of their own religious belief or sect.

Intelligence

Since the fall of the Soviet empire, we have witnessed a decrease in activities in the intelligence communities. As a result, our need to have intelligence on the ground has never been more critical than it is today. On a daily basis, we are seeing reports of possible terror cells . . . or links to them being uncovered. This is only happening because massive resources are now being applied to the intelligence apparatus. The intelligence communities, both at home and abroad, jealously guard the information they gather and often do not share willingly with their own law enforcement and security agencies or allies on a regular basis. This must change. Obviously, the need to acquire and disseminate intelligence within North American agencies has never been more critical. With the ending of the Cold War era, the need for covert actions conducted by the CIA was on the wane due in no small part to the erosion of budgets for "in the open" and covert intelligence activities abroad. It must be noted that covert action in pursuit of a political agenda and foreign policy dictate tends be become somewhat controversial. Covert actions are tools of the Presidency, and therefore, they do have a political resonance. They are executed by an agency (the CIA) that is under the direct orders of the President and the National Security Council.[5] The establishment of homeland security efforts in the United States will no doubt add to the efforts to protect society and detect and deter terrorist acts against western society. Legislation currently being introduced will address new and sweeping powers for both police and security agencies. In addition to the lack of current human intelligence resources, there is a balance in signals intelligence between developing new systems and technologies to penetrate more complex communications without forgetting how to decode the old systems of encryption.[6]

International intelligence gathering is centralized through Interpol. Interpol's involvement in the fight against international terrorism materialized during the 54th General Assembly in Washington in 1985 when Resolution AGN/54/RES/1 (Washington, DC, 1985) was passed calling for the creation of a specialized group within the then Police Division to ". . . coordinate and enhance cooperation in combating international terrorism . . ." The same resolution also called for the preparation of an instruction manual "outlining the practical possibilities that currently exist for cooperation in dealing with terrorist cases."

Criminal intelligence analysis, however, began in North America. In the 1960s, organized crime became a real threat to society and was described in the President's Crime Commission report on the "Task Force on Organized Crime." The conclusions of this report stated that law enforcement was ineffective in its approach to organized crime. As a result, many intelligence programs have since been developed. One of these is the Anacapa Science Program, which has provided the basis for certain criminal intelligence analysis techniques. Criminal intelligence analysis uses uniform techniques focusing on the development of hypotheses, reconstructing the course of individual criminal incidents, identifying a series of related crimes, understanding criminal networks, and analyzing the scope of and patterns in criminal activity. Criminal intelligence analysis techniques provide a standardized approach yet offer flexibility that is limited only by the ability and imagination of the crime analyst. Crime analysts are frequently limited in number, so they usually work on larger or more complex cases and projects.

Existing and new techniques are constantly being developed in order to extend the range of investigations and projects on which they can work. Operational analysis has been explored and proven to be an effective tool in investigations. In the 1990s, strategic forms of criminal intelligence analysis were more fully explored, and crime pattern analysis also became a well-used method for policy making. As criminals move into different areas of crime and their methods become more sophisticated, it is important for law enforcement agencies to be able to adapt their own methods.

Criminal intelligence analysis has been recognized by law enforcement as a useful supporting tool for 25 years now. Recently, criminal intelligence analysis has also been recognized as an important additional support for international cooperation in police matters. Such cooperation can be bilateral and/or multilateral. Criminal intelligence analysis has found its role in both situations and is therefore highly recommended. Countries with great experience in criminal intelligence analysis and international law enforcement organizations should continue with these efforts. Naturally, ICPO-Interpol is not an exception to this: it produces and offers professional analytical reports to its entire member country network in the best possible manner. Next to this, it is also offering technical advice, comprehensive manuals, and professional training in the technique.[7]

Interpol's multinational police cooperation process has a three-step formula for dealing with terrorism, a formula all nations must follow: (1) pass laws specifying that the offense is a crime; (2) prosecute offenders, and cooperate in other countries' prosecutions; and (3) furnish Interpol with and exchange information concerning the crime and its perpetrators.[8] The challenges for the intelligence community are enormous—uncovering "sleepers" currently residing in both urban and rural settings is crucial to disrupt and prevent the next attack, as there seems little doubt that we must expect another attack. The process of profiling is made more difficult when one appreciates how global the Osama bin Laden group actually is and how far reaching are its tentacles. In this regard, there are trained supporters currently with the Islamic Movement of Uzbekistan located in Tajikistan and Uzbekistan. In Lebanon with Hizballah (the Party of God), this group has long been associated with the Shi'a fundamentalist group in Iran and is allied with al Qaeda in the many training camps of the Middle East. Nearer to home, the threat comes from the Philippines where the Abu Sayyaf Group (ASG), translated literally meaning Father of the Executioner, Bearer of the Sword, resides. It was this group that was aligned with Ramszi Yousef (1993 WTC bombing). An equally dangerous and threatening group is based in Algeria with ties to Montreal Canada. The Armed Islamic Group (GIA) had many members fighting in Afghanistan against the Soviet Union as Mujahideen. Many links have been made between this group and conspirators based out of Montreal. In Egypt, al-Gama'at al-Islamiyya is violently opposed to the secular government of Hosni Mubarak. The truly global nature of the terror threat cannot and must not be confined to profiling of an ethnic group. The global nature of the organization means that greater efforts and communication must come from intelligence communities around the globe. It has obviously been easy for us to criticize the intelligence community as a whole for the failure to detect or disrupt the September 11 events. As Pogo stated, "Predicting stuff is difficult, especially if it's in the future."

Case Study

It is sometimes strange and often disturbing how, with apparent ease, the terrorist is able to launch an attack. Witness if you will the mortar attack by the Irish Republican Army at London's Heathrow airport in March of 1994. Airports are likely to remain symbolic, literally terror-inducing targets, and I feel sure that there are useful long-term lessons to be learned from this series of incidents and the way in which they were handled. It is also important to bear in mind that this attack at Heathrow, one of the busiest airports in the world, was only one small part of a terror campaign that had been ongoing since 1972. The terrorists interspersed hoax calls with deliberately imprecise, inadequate warnings followed by bombs. A key aspect of police strategy developed over many years is to strike a difficult balance between public safety, which must be viewed as paramount in our free society, and overreaction, which can result in paralysis to transport systems. A condition that, in itself, can have serious implications for public safety.

The first attack took place after coded telephone calls were received at around 5:00PM warning of "bombs and explosions at Heathrow, in terminals and runways in one hour." An explosion in a vehicle on the north side of the airport in the parking lot of the Excelsior Hotel took place at around 6:00PM. Hotel parking lots were habitually used as evacuation staging areas. The second and third attacks took place the following evening and three days after that. The weapons used were homemade mortars with the aerodynamic characteristics of a brick, fortunately. One can imagine the disruption that these incidents caused to transportation! The lessons learned from this incident reveal two key principles:

1. The more effective security within airports increases the risk that terrorists will look to locations outside airport perimeters from which to mount their attacks. There can never be total, impregnable security.

2. The value of interagency cooperation cannot be overemphasized.

The review identified four aspects worthy of note in respect to security arrangements:

1. The prior identification of vulnerable areas

2. Frequent review of contingency plans

3. Greater use of CCTV

4. Working with the media

On the basis of aerial photography and mortar base plate surveys, police should draw up graded risk, contingency plans, identifying vulnerable locations and potential firing points. Police must look more closely at identifying who owns or occupies the land surrounding the airport. The review also identified that a coordinating group system for the management of security alerts is also essential. In addition, the use of CCTV should be effectively monitored and be of sufficient standard for evidential purposes.[9]

The Biological Threat

Biological weapons are more deadly and financially efficient, pound for pound, than chemical agents or even nuclear weapons. Ten grams of anthrax could kill as many as a metric ton of the nerve agent Sarin could.[10]

Biological threats and attacks against civilians are not confined to an anthrax episode/scare such as those being currently witnessed. The United States has been previously targeted for biological attack. That episode took place in Dalles, Oregon in 1984 when an obscure sect led by a Guru from India contaminated the food in a number of local restaurants by spiking the food bars with salmonella bacteria. More than 750 local residents became severely ill as a result. Governments as far back as World War II have contrived programs for the use of biological agents. The sarin gas attack by the terror group Aum Shinrkyo on a Tokyo subway station also uncovered evidence at the terrorists' camp that they were equipped with anthrax and a crop spraying helicopter, presumably as the means of deployment. That society is vulnerable to a biological attack is indisputable; however, the problem this raises is that the targets are also limitless. Although the anthrax attacks, albeit small in number, could have similarly been an attack against the country's livestock population, the resulting livestock loss would have had a significant effect on the economy and also on freedom of travel. The opportunity to introduce biological agents is almost unlimited in this respect. The problem here is only after the introductions of the agent do we become aware that an attack may have taken place.

Anti-Terror Organizations

In the war on terrorism, it falls to law enforcement to be the arm and the instrument of government to defend the nation at home. Of concern to many will be civil liberties and how much society is prepared to sacrifice to achieve freedom from terror, but we cannot forget that the threat to the U.S. is not purely restricted to international terrorists. There are many survivalist groups, white supremacists, or neo-nazis who will view any attempts to restrict freedoms as cause for a call to arms. From a policing standpoint, the U.S. has many well-trained and equipped specialist units be they Seal Teams, Delta Force, or Secret Service Agents. Whether they be members of military or police units is irrelevant; however, the challenge may come down to one of jurisdiction.

Anti-terror units came about as a reality in Europe with the explosion of terror attacks against European interests in the late 1960s and 1970s. Jurisdiction for the upcoming Winter Olympic Games will be a major test of the capability and capacity of the U.S. to defend and deter against terror attack. The Munich Olympic Games massacre stands as a symbol of how a devastating attack by a fanatical terror group, in this instance Black September, can have deadly consequences for the protagonists and the participants. As a result of the failed rescue attempt by West German Police, the government recognized its own lack of preparedness to deal with such hostage-taking incidents. The unit GSG-9 was formed under the direction of the West German minister of the interior. Looking to establish an elite corps to handle all terrorist activities on a national basis, the Federal Border Police who were paramilitary formed the basis of the 188-man structure. GSG-9 began training in 1972 under the leadership of Ulrich Wegener, a terrorism expert in his

own right. It was originally organized into three strike units backed up by other support units, including an HQ, communications and intelligence unit, engineer unit, research and equipment unit, maintenance and supply unit, and training unit. The West Germans realized that intelligence is a key part of anti-terrorist operations, and GSG-9 was hooked into the giant computer system in Wiesbaden.[11]

In similar fashion to the British Special Air Service Regiment (SAS), selection testing and training is rigorous to say the least. While the activities of GSG-9 at Mogadishu in 1977, the SAS at Princes Gate London, and Israeli Special Ops actions in Entebbe in 1976 are the stuff of legends, the U.S. as well as all other governments must now focus on how to prepare for the next round of terror tactics. Currently, the U.S. has a great many units trained to various levels of effectiveness to handle the growing trends in a violent society, but are these units prepared for terror operations and the necessary response at home? The likely answer is probably not. Here ultimately is an opportunity for the Office of Homeland Security to take charge and give some much-needed direction to a national unit to respond to terrorism without the trappings of local, state, and national politics interfering. It is therefore clear that the decisions on jurisdictions for a national unit to respond to terrorism; be it police, military, or a combination of the two; must be resolved.

The best anti-terror units in the world today can only be effective if they can be brought into action quickly and with a clear directive. Civil libertarians have balked at some of the responses that have already been meted out to terrorists. The rescue of hostages in the Iranian Embassy in Princes Gate, London showed to powerful effect how a highly trained and directed unit rescues the hostages which was the number one priority, but the elimination of the terrorists in swift brutal fashion had libertarians asking the usual questions about shoot-to-kill policy and sanctioning of assassination. In the Iranian Embassy, the SAS was sent to rescue the hostages not to arrest anyone. Normally, dead terrorists are better than live terrorists since they are no longer available to cause other terrorist acts in an attempt to free them from prison.[12] Again, the ruthless nature of anti-terrorism was illustrated by the SAS in its tracking of an IRA unit to Gibraltar in 1988. Intelligence reports indicated that the cell was about to detonate a bomb during a military parade. The SAS carried out an attack on the three IRA members and, according to witnesses, gunned them down in cold blood. The subsequent outcry seemed too much for a democracy to handle, with claims of a government "shoot-to-kill" policy. The IRA now had martyrs to bury at home in Northern Ireland and the opportunity to haul the British government before the European Court of Justice, which condemned the assault. This court decision showed that caution was required, lest counter terrorist forces go too far. Of course for the IRA, it meant that they had the right to not only shoot first, but to kill as well!

In conclusion, terrorism is a complex, multifaceted, and often baffling subject. The players involved have a way of rising to prominence, splintering, disappearing for years, and then reappearing. Counter-terror bureaucracies are formed and then reformed; names are changed. Leaders are shuffled around as they are promoted, demoted, or forced to resign. Incidents proliferate across the world, some of which can trigger a chain of events that will destabilize a whole region and bring nations to the brink of ruin. At the same time, major terrorist actions can shock for a short while and then be quickly forgotten (except of course by those effected by

the tragedy). Treaties are written, theories propounded, grievances aired, tactics discussed, occasionally to some effect, usually not.

The threat posed by terrorism has been transformed. In essence, the threat of terrorism is presently intensifying in direct relationship to political, social, and economic situations occurring outside the United States. Gratuitous violence will continue to be a goal of the terror organizations as long as they view it as a means to their ghastly end. As for law enforcement and counter terrorism, the new Office of Homeland Security under the control of Governor Tom Ridge must have final authority and accountability. There are currently more than 40 agencies now sharing responsibility for domestic security, which in turn spreads the accountability too thin. The Office of Homeland Security is the opportunity with support of congress and the President to take the first major steps in protecting the citizens of the U.S. Civil libertarians will no doubt suggest that the legislation is too far reaching, giving too many new powers to law enforcement. These are dangerous times, calling for drastic measures to protect our society. This struggle, this war will continue for many years to come—over time, we will be able to better assess how successful the new legislation will be. I trust that time will not diminish the horrific events of September 11 and the reasons that such harsh legislation is now necessary.

Major Legislation Resulting from September 11th Terrorist Attacks

HR2882: Public Safety Officer Benefits Bill

HR2884: Victims of Terrorism Relief Act of 2001

HR2888: 2001 Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States

HR2926: Air Transportation Safety and System Stabilization Act

HR2975: Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001 (Replaced on October 12, 2001 by HR3108, the "Uniting and Strengthening America Act" or "USA Act of 2001," which closely mirrors the Senate anti-terrorism bill, S1510)

HR3016: Amending the Anti-terrorism and Effective Death Penalty Act of 1996

H.J.Res. 61: Expressing the sense of the Senate and House of Representatives regarding the terrorist attacks launched against the United States on September 11, 2001

H.J.Res. 64: Authorization for Use of Military Force

S1424: A bill to amend the Immigration and Nationality Act to provide permanent authority for the admission of "S" visa non-immigrants

S1426: 2001 Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States

S1447: Aviation Security Act

S1450: Air Transportation Safety and System Stabilization Act

S1510: Uniting and Strengthening America Act (USA Act of 2001)

S.J.Res. 22: A joint resolution expressing the sense of the Senate and House of Representatives regarding the terrorist attacks launched against the United States on September 11, 2001

S.J.Res. 23: Authorization for Use of Military Force

Endnotes

[1] Wright, R. (1986). *Sacred rage.* New York: Simon and Schuster.

[2] Ibid.

[3] *Jane's Intelligence Review* (July 2001).

[4] Hoffman, B. (1998). *Inside terrorism.* New York: Columbia University Press.

[5] Cogan, C. G. (1993, April). Covert action and congressional oversight: A deontology. *Studies in Conflict and Terrorism*, *16*(2), 87-97.

[6] Hill, S. *Crime and Justice International, 17*(56).

[7] Interpol Website – The Internet

[8] Peak, K. J. (2000). *Policing America* (3rd ed.). Englewood Cliffs, NJ: Prentice Hall.

[9] Tucker, D. (1994). *Metropolitan police*. Extracts from a presentation to AVSEC World Symposium 1994, Chicago.

[10] Maniscalco, P. M., & Christen, H. T. (2002). *Understanding terrorism and managing the threat*. Englewood Cliffs, NJ: Prentice Hall.

[11] Thompson, L. (1986). *The rescuers: The world's top anti-terrorist units.* Boulder, CO: Palladin Press.

[12] Ibid.

Jeremy Spindlove is a former British police officer who was involved in the IRA pub bombing campaign in the early 1970s. He went on to work in a security management capacity for British Airways and saw terrorism at first hand while stationed in Baghdad, Beirut, Jordan, and Egypt. He is the former Director of Security for the Vancouver International Airport Authority in Canada and is the coauthor of a text on terrorism titled *Terrorism Today, The Past, The Players, The Future*, published by Prentice Hall in 2000.

Terrorists, Enemies of Mankind

Peter J. D'Arcy, LLB
Police Advanced Training, Justice Institute, BC

Introduction

Before we try and deal with terrorism, I would suggest that we must first understand the phenomenon of what terrorism is. It is common knowledge that there are two types of terrorism: one is domestic in nature and the other international. Both share similarities and yet are quite distinct. This article addresses the issues surrounding international terrorism, specifically, Middle Eastern terrorism and its connection to Islam, the world's fastest growing religion. It may also be helpful at this early stage to draw an analogy with the law enforcement approach to dealing with organized crime. For example, when law enforcement personnel identify hard criminal targets, either an individual or groups, they tend, as a first step, to carry out detailed background checks, including a personal history of the targets. The same approach is necessary when dealing with terrorists; however, the difference is when carrying out their background checks, law enforcement personnel tend to deal with a variety of different agencies and a variety of information. To truly understand Middle Eastern terrorism, I would suggest that law enforcement personnel should also have an understanding of the history. I would further suggest that we may have to go back as far as 2,000 years in order to understand the present. This may cause the reader to ask the question, "Why look back so far?" One reason is to identify with the rich successes enjoyed by different Middle Eastern groups who have employed terrorism and benefited from its use for literally that long. The Middle East is where our main threat resides today. In fact, a recent edition of *Time* stated that the Popular Front Liberation Palestine-General Command (PFLP-GC) are active again since the September 11 attack in New York.[1] The PFLP-GC are a group, infamous for hijacking three civilian airliners in 1970, flying them to Dawsons Field in the Jordanian desert, releasing all the passengers and crew, then simultaneously blowing up the aircraft.[2] Their reappearance may or may not be significant, when we consider that Osama bin Laden has allegedly been attempting to unify other terrorist groups to join al Qaeda. The September 11 attacks have gone way beyond previous levels of violence and may be seen as a signal or rallying call, not only to unite, but also to step up the levels of violence by other groups. Secondly, law enforcement personnel should be aware that, historically, anniversary dates have played a significant role in Islam. Finally, terrorists (or freedom fighters) from the Middle East have historical ties to suicide and martyrdom, which is seen by some as a joyful act which in turn is strongly associated to the beliefs and faith of some Muslims, particularly in Lebanon and Iran.[4]

President Bush has said that the war on terrorism is not a war on Muslims or Islam; I have no reason to doubt him. This statement may be a true reflection of the President's intentions. The President said that the war is only directed at those terrorists who attacked America. He described them as people who would use the religion of Islam to try and legitimize their acts of war. This strategy, he says, is also intended to bring together Muslims from all over the world and lead them into a Holy War or Jihad.[5] When considering the term *Jihad* and in order to clear up any ambiguities, it should be noted that *Jihad* does not mean "holy war." It

means "to struggle," and the struggle according to the Islamic Bible, the Koran, means simply to be a good Muslim and to support the Five Pillars of Islam, which are basically to struggle on this earth and be a good and holy person, which includes but is not limited to fasting for the month of Ramadam, praying five times a day, giving alms to the poor, visiting Mecca on a pilgrimage, and recognizing that there is only one God, Allah, and only one prophet, Mohammed.[6] I suggest, however, that of the 650,000 Muslims who reside in Canada and the four million who live in the United States, and the remainder of almost one billion Muslims who reside around the globe, some of them do perceive *Jihad* to mean "holy war" and the United States and its allies as aggressors and do indeed see this war on terrorism as a struggle against Islam. It is these Muslims who have deliberately extended the meaning of Jihad to include "holy war" as part of the struggle[7]; therefore, we can claim in the West that it is not a war on Islam, but amongst some Muslims, there are many thousands who would claim the opposite is true, as the recent riots and attacks on non-Muslims in Pakistan and the Philippines have testified.[8] We have recently seen and experienced on September 11 what only 19 of these young men from the Middle East have achieved, including recognition as martyrs by some.

I would not suggest that they have brought the world to its knees, but I would suggest that they have made the world sit up and pay serious attention to, among other things, the Palestinian situation, one of a series of problems that have been present in their world for many years. I would further suggest that it is the deeply entrenched cultural belief system of these Muslims, which is diametrically opposed to Western standards and Western-held beliefs, that has led us into an arena of misunderstanding and conflict that has explosive potential. The most extreme example of this cultural difference is to try to understand what makes the terrorist so deadly. Succinctly summed up by a world-renowned terrorism expert, Professor Paul Wilkinson of St. Andrews University, Scotland, when he quotes Leon Trotsky, "It is not the terrorist's capacity to kill, but indeed, his willingness to die."[9]

Even though acts of terrorism can be traced back 2,000 years, the terms *terrorism* and *terror* are of relatively recent date. The first recorded meaning of *terrorism* was given in the 1798 supplement of the *Dictionaire of the Academe Francais* as *system regieme de la terror*.[10] According to a French dictionary published in 1796, the Jacobins used the term when speaking and writing about themselves. *Terrorism* became a term of abuse with criminal implications.

A Brief History of Terrorism

One of the earliest examples of a terrorist campaign dates back to 66 AD to 73 AD with a highly organized religious sect known as the Sicarri, consisting of men of the lower orders active in the zealot struggle in Palestine. They used unorthodox tactics such as attacking their enemies on holidays when crowds congregated in Jerusalem. They would select a random and innocent civilian victim and stab him or her to death in the crowd. The fact that they chose innocent civilians meant that no one was safe and, therefore, induced fear in a target group beyond the actual victims and their families. This had the effect of spreading fear beyond the intended victim and having an influence on those to whom the message was really directed. Victims rarely count in the equation where terrorism is concerned.[11]

The Sicarri regarded martyrdom as something joyful, and it suggested that their actions were no different from what the world witnessed on September 11. In the 11th century, for almost 200 years, the assassins, who were an offshoot of the Ismaili community, spread fear by killing prefects, governors, and caliphs. Originally based in Persia, or as we know it today, Iran, they spread throughout Syria to Palestine. Their leader, Hassan Sibai, recognized that his group was too small to confront the enemy in open battle but carried out a planned, systematic reign of terror with a small but well-disciplined force who were prepared to die for their beliefs.[12]

They, too, viewed martyrdom as something special and joyful. The assassins only used a dagger; for them, murder was considered to be a sacrificial act. Even if we consider some European examples of terrorism, they, too, can be identified by the same traits.

During the Camisard Revolt which shook Europe in the Spanish War of Succession in the early 1700s, French peasants seized a number of pregnant Catholic women as symbolic targets and slew them, tearing the unborn fetuses from their wombs, thus using extra-normal violence, and again having the obvious effect of spreading fear beyond the actual target victim into the larger community.[13]

Many countries have had their Siccari and assassins, Sicilian vespers, and other foes. As a tactic, therefore, terrorism has persisted through the centuries. The idea and tactic has evolved to become the modern, sadly sustained phenomenon we explore today. We can also see that modern terrorism has a history with many examples of success. From the Russian revolutionaries such as the Narodanaya Volya who employed the same strategies of terrorism which carried us into the 19th and 20th centuries[14] to today's Arab terrorists who try to link their activities to both political and religious ambitions. Because Islam is a way of life for these terrorists, both religion and politics are inextricably tied together, and for most Muslims, they cannot be separated. If we asked any moderate Muslim, however, if the actions of September 11 would be acceptable in the Islamic faith, they would first ask for proof. If proven, they would denounce those responsible for such acts and hand them over to face justice, and justice for such acts in the Islamic faith is death. Throughout the 20th century, many other groups have emerged—for example, radical nationalists such as the IRA, Aryan Nation, Macedonians, Serbs, and Armenians; Marxist revolutionaries such as the Italian Prima Linea Group; Social Revolutionaries such as the American Black Panthers; political theorists such as the Autonomia Movement of Italy; the PLO and the 40 or so splinter groups that it has spawned such as the PFLP-GC, the Eagles of Palestine, and the Black September group who attacked the Munich Olympics in the 1970s. It is estimated that by the mid- to late 1980s, over 1,000 terrorist groups had claimed credit for more than 8,000 terrorist events.

The Present

As we can see, terrorism has a long history. It has enjoyed almost continuous success when employed. It has never been fully stopped. It cannot be killed or imprisoned. It evolves constantly. In the 1970s and 1980s, it gave us Abu Nidal, Hamas, Hizbollah, Islamic Jihad, etc.; and today, it gives us bin Laden and al Qaeda. That's not to say that those other groups have disappeared. Some are just more active than others at different times.

Definition

As mentioned above, there are basically two types of terrorism: (1) domestic and (2) international. If we consider domestic terrorism, this would include disgruntled individuals such as the Unibomber or groups such as the Animal Liberation Front or the Aryan Nation (though its activities are domestic, it is an organization that has thousands of members around the globe) who influence the Timothy McVeighs of the world. People who either individually or as a group possess enormous destructive capabilities and who only require two things to become deadly: the Will and the Means.[15] One other point worth mentioning is that when a major terror campaign is launched by big players, such as international terror groups like al Qaeda, law enforcement personnel need to keep an open mind because it is at these times that the smaller fringe groups of anarchists sometimes "piggyback" on the shirt tails of the main players. This is done with the intention of letting the blame fall on the big players even though their activities are far less dramatic, but the desired outcome is still the same: destabilization of the government and the society it represents. It should also be said that domestic terrorism is more easily defined and criminalized. It can be dealt with internally, within each nation state such as the British Prevention of Terrorism Act of 1974 or the pending Canadian anti-terrorist legislation of October 25, 2001, or the new U.S. anti-terrorist legislation.

International terrorism, however, is far more complicated. Though easy to describe, it has never been given a universally accepted definition. This, in turn, inhibits the ability of the states to define a universally acceptable definition of terrorism, which, in turn, has historically inhibited our ability to legislate and respond on a unified front. That is until September 11.

Terrorism has many faces, most of them invisible! It has eluded complete understanding for decades. This confusion can be traced to its earliest roots 2,000 years before. It crosses the boundaries of many considerations and disciplines, including the religious, political, legal, military, psychological, and social spectra.

Entire doctoral dissertations have failed to define the phenomenon.[16] Academics have identified that there are 22 recurring elements, but not all of these are always present. Of these 22 elements, some recur more than others. It has been estimated that the United States has expended as much as 18,000 man years in research time on this phenomenon alone.[23]

Finance

International terrorism has a huge reservoir of funds to finance its terrorist campaigns. The money comes from many sources, including organized crime, NARCO terrorism, and huge financial gifts from certain sympathetic oil rich states. In the mid-1980s, for example, the PLO had an annual income of $1.25 billion from its investment income alone. Gifts were often given by wealthy, oil rich states to support the causes, so long as the terrorist activities took place far away from the gratuity granting state. The support and sympathies for such organizations allegedly went beyond just financial contributions. In fact, as many as 19 states have even extended their support to include asylum to aviation hijackers. Some terrorist organizations resemble Fortune 500 companies, including pensions, bonuses, and

employee assistance programs.[17] There is even an association for martyrs. Suicide bombers have an actual registered association in Beirut for taking care of the families they leave behind. They are not considered to be terrorists; on the contrary, they are considered to be martyrs and heroes. They are so revered that their pictures are displayed all over the city. Sadly, there is no shortage of these people who believe in martyrdom. It is suggested that the distinction between terrorist and martyr/freedom fighter may be defined by the type of target chosen, military or innocent civilian. Either way, it is this kind of funding which allows the individuals and or groups the ability to create complex, productive infrastructures. The funds also allow them enormous flexibility to buy first class air travel, complete dry-runs, pay informants, and set up safe houses and support networks such as for obtaining false documents and vehicles. One of the biggest indictments of our false sense of security, however, is that we have allowed such organizations associated with terrorism to set up offices in our own countries.[18] Organizations that have been soliciting financial support for these causes are among us here today!

In Canada, there are 50 known terrorist groups that have been identified. In the United States, groups can be found from the east to west coasts and include Hamas, Islamic Jihad, Hizbollah, Muslim Brotherhood, National Islamic Front, Algerian Islamic Front, and the Muslim Brotherhood of Osama bin Laden, as well as hybrid fundamentalist groups[19] and many splinter groups. Therefore, when we compare these kinds of odds and financial resources to the government spending and budget for fighting terrorism, our efforts seem almost meaningless and certainly impotent. Historically, we have become reliant on security services such as CSIS, the CIA, MI5, and MI6—organizations that have all suffered staffing and financial setbacks and must operate within the rule of law. Wilkinson cautions against dealing with terrorists using the everyday norms of Western liberal democracies. These agencies have enjoyed limited success in establishing productive intelligence, which is, I would suggest to you, our first line of defense. I am not just referring to spy intelligence activities, but the kind of intelligence that could be generated by front line law enforcement agencies from simple things like traffic stops, domestic calls, and so on. Terrorists drive cars; terrorists speed; terrorists have domestic disputes just like everyone else. Just think of how Timothy McVeigh was caught . . . It was a traffic-related stop. Mohammed Atta, who is suspected to be one of the pilots who steered a plane into one of the two World Trade Center Towers, was stopped for a driving infraction in South Carolina just prior to the September 11 attacks. He was on the FBI's watch list, but the information never made it to the street-level officers. There is a dire need to provide not only intelligence training to such front-line officers, but to create provincial and state, national, and international reporting procedures. Such reporting needs to be standardized to ensure accuracy of reporting standards. It is also necessary to ensure use of the same standardized language and terminology to make such unified response across our countries a success. I further suggest that to rely solely on the intelligence agencies would be, under these present circumstances, a gross miscalculation on the part of the authorities.

It is not easy to profile these terrorists. They are often well-educated, many in the West. They are not poor. They have money. They are not socially inept, and they fit nicely into Western society. We can, however, potentially profile their activities, whether it is the way they purchase airline tickets, how they obtain official documents such as drivers' licenses, or how they go about their daily activities such as setting up businesses.

Media and the Lessons of Tite Street

Today, more then ever before, the media has become a huge player where terrorism is concerned. I, for one, have a great respect for the potential and power of the media; I support the concept of freedom of the press to report events because the positives have normally always outweighed the negatives. Where the latest trends in terrorism are concerned, however, I suggest some restraints may be necessary, particularly at the actual scene. Dangers always exist when reports are allowed to be published unchecked.

In the early 1970s in London, England, a bomb was placed and detonated in Tite Street. The appropriate law enforcement authorities, including specialist units, attended the scene. Unknown to those first responders and specialists, a second remote controlled device had been placed in a mail box. The media arrived at the scene with TV cameras and started to film and report. What was also unknown was that the terrorist group responsible for the incident was close by in an apartment watching TV. When the number of law enforcement personnel increased and were close to the mail box, it was detonated, innocently aided by the media. This is a lesson that is worth sharing and should be given consideration if your department becomes involved at a scene.

The Picture Today: Some Important Facts

If we take a moment and examine bin Laden and his organization, al Qaeda, and consider that they are one of the wealthier terrorist groups, we may agree that they are a formidable opponent! Bin Laden is the 17th son of 52 children born to a Saudi billionaire. He has been a radical and freedom fighter since 1979. He is rumored to be worth some $300 million. He has established support networks in the Sudan and Afghanistan.[20] In the year 2000, he was reported to have visited al Qaeda members in Albania.[21] He is revered by many Muslims worldwide. His objective is to rid the Middle East of all American influence; to return Palestine to the Palestinians; and to overthrow the Saudi Royal Family, taking control of the two most Holy places in Islam, Mecca and Medina. He has reportedly succeeded in either uniting or stimulating interest from several terrorist organizations; al Qaeda is reputedly 5,000 strong with people in over 60 countries worldwide. He has been involved in these efforts to unite the Middle East and achieve these goals for over 20 years. In 1993, al Qaeda allegedly tried to obtain components of nuclear materials to begin work on chemical weapons for development in the Sudan. In 1998, it was reported by the Arabic newspaper *Al Hayat* that bin Laden had acquired nuclear weapons from Soviet Central Asian countries. One such area to purchase armaments and other equipment is an area known as Vedanka outside the Cosmos Hotel in Moscow, an area similar to the PNE in Vancouver, Covent Garden in London, or Coney Island in New York. Anthrax was offered openly on the street for sale. At a recent police conference in Montreal, British police sources revealed that illegal immigrants attempting entry to the UK had been caught in the Channel and, when intercepted, were found to be in possession of vials of anthrax. During the Cold War, the Soviets manufactured between 80 and 100 tons of smallpox per year as a weapon. Since Glasnost and the Berlin Wall coming down, according to intelligence resources, many of these biological weapons have remained unaccounted for and, like anthrax, are suspected of being sold on the world's black markets. In 1999, the United States directed an attack on a pharmaceutical company in Sudan suspected to be manufacturing biological and chemical weapons. This plant had suspected links to al Qaeda.

In the past 24 months, there have been 423 recorded terrorist attacks worldwide; 200 were anti-American in nature, culminating in 2001 with the attacks on the World Trade Center and the Pentagon, leaving approximately 7,000 civilians dead. In response to September 11, 580 people have been arrested worldwide, including individuals in France, Spain, the United Kingdom, the United States, and Germany. The FBI is working flat out on some 300,000+ leads, which any investigator knows is almost an impossible task to complete in a timely and useful fashion. This alone poses a further question: "How does law enforcement keep up with these activities when using traditional investigation methods?" September 11 is just one series of attacks, being further compounded by anthrax attacks. How will the FBI cope with a second and third series of attacks from an investigation perspective? It is now known that some of these arrests interrupted other planned terrorist attacks in Europe, including the American Embassy in Paris. Of those suspects arrested, some were Algerian, United Arab Emirates (UAE), and Saudi citizens.[22] Alleged terrorist funds have been seized in Norway and the UAE. In addition, security services foiled another al Qaeda attack when a hijacked Air France airliner was en route to be flown into the Eiffel Tower in Paris prior to the September 11 attacks. The magnitude of responses to a series of potential terrorist attacks is almost unimaginable, as history has shown us.

Recommendations

It is suggested that the first line of defense ought to be a universal and standardized form of intelligence training for all personnel, as it is intelligence gathering that offers promise of success in preventing future terrorist attacks. This intelligence will only be effective, however, if there is standardized reporting at the provincial and state levels to a centralized, coordinating body within the federal system to disseminate this information to appropriate specialist units and, in turn, to our allies. This is a practice that may be less than perfect, particularly between internal security services. Sharing of such information is subject to obstacles that range from petty jealousies and rivalries to legislation that forbids such revelations. Other training recommendations include full-scale simulation training dealing with conventional terrorist attacks, nonconventional nuclear bio/chemical attacks, and the creation of a communications network encompassing not only emergency services personnel (who deal with people) but extended to organizations such as the SPCA, private veterinary clinics, agricultural organizations, and transportation systems. The United States' formation of a Homeland Defense Bureau is an excellent example of a first step in resolving the critical problems associated with the sharing of information.

Finally, in order to guarantee any level of success, there is a need to create legislation that will require appropriate reporting procedures and collaborative efforts, implemented nationwide and internationally.

Conclusion

In conclusion, the United States and its allies have gone to war, yet the Muslim world has asked for proof and has offered to give up bin Laden upon production of such proof. According to the Koran, he should be put to death once proof is provided. As one senior Arab police officer recently confided, "Give us the proof, and we will deal with bin Laden." Surely this is an area that needs to be explored;

it would certainly appease those who seek justice if not revenge. After all, any court would require law enforcement officers to satisfy this standard on a daily basis. Many people and agencies are being carried along on an emotional roller coaster. Is it unreasonable to ask why the evidence is being held back? Why not just give the Muslim world an opportunity to see the proof and act on it? The alternatives seem almost too horrible to imagine. As mentioned from the outset, if we are to prepare our front line law enforcement and emergency services personnel, it is imperative to consider the theories of terrorism, the history of terrorism, and the complexities that characterize the phenomenon. Terrorism by its nature has historically been successful and never stopped; it continues to evolve. September 11 is its legacy!

It is not the terrorist's capacity to kill, but indeed, his willingness to die.

Leon Trotsky

Endnotes

[1] *Time* Magazine (2001, October 27).

[2] Harris, cases and materials on International Law.

[3] BBC, Tuesday, September 18, 2001.

[4] "Target America," *PBS Frontline.*

[5] CNN News reports, October 7 to 15.

[6] Haneef, S. (1979). *What everyone should know about Muslims and Islam*. Pakistan: Kazi Publications, p. 118.

[7] Ibid, p. 119.

[8] *National Post* (2001, October 29), p. A7.

[9] Wilkinson, P. (1986). *Terrorism and the liberal state* (2nd ed.). New York: Macmillan, p. 247.

[10] *Terrorism and political violence* (Vol. 1, p. 54). (1989, January). London: Frank Cass.

[11] Brandon, S. G. F. (1967). *Zealots, Siccari and Rome*. Manchester, England: Manchester University Press.

[12] Lewis, B. (1967). *The assassins: A radical sect in Islam*. Oxford, England: Oxford University Press.

[13] Bray, A. E. (1870). *The revolt of the protestants of the Cevennes 1870*.

[14] Wilkinson, *Terrorism and the liberal state* (2nd ed.) (1986).

[15] *The Times* (1976, December 13). (L.A. County Sheriffs found an 8 ton cache of munitions in the desert 60 miles north of L.A. They also found anti-black anti-semitic literature as well as medical supplies and chemicals for making Napalm and poison gas.)

[16] Schmidt, A. P., & Jongman, A. I. (1983). *Political terrorism*. Amsterdam: North Holland Pub. Co.

[17] Adamson, J. (1986). *Financing of terror*. London: New English Library.

[18] Dobson, C., & Payne, R. (1979). *The weapons of terror*. New York: Macmillan Press.

[19] Emerson, S., Director. (2001, September). *Terrorism Newswire*. Washington, DC.

[20] BBC, *News and Panorama Documentary*, Tuesday, September 18, 2001.

[21] CNN News reports, November 10-20, 2001.

[22] CNN News reports, October, November 2001.

[23] The First International Seminar on Aviation Security, Tel Aviv, Israel, 1989.

Peter J. D'Arcy, LLB is a former operational member of Scotland Yard's Anti-Terrorist Unit. He has also worked with the 21st Special Air Service Operations Intelligence Section. He spent considerable time in and dealing with the Middle East. He has contracted security services with several Middle Eastern Embassies. He has spent several years engaged in post-graduate research on terrorism. Currently a member of the Vancouver Police Department, he is currently on secondment as faculty at the Justice Institute of BC.

The views expressed in this article are the views of the writer only and are not the official views of any agency or organization.

Terrorism: Nothing New – A Predictive Model for Handling Terrorist Incidents

Robert J. Fischer, PhD
Bruce Heininger, PhD
Lieutenant Colonel Fred Berger

The research for this article was completed in the early 1980s; however, the models that were developed at that time have as much application to our present situation as they did when first developed. The article is dedicated to the memory of our dear friend, Dr. Bruce Heininger, who departed our company this year. Bruce was a dedicated law enforcement professional, who tried to make life better for all.

While the recent events of September 2001 have brought the reality of terrorism to American soil, terrorism is not something new. Law enforcement and security professionals have been studying this tactic for many years. Unfortunately, support for anti-terrorist strategies had not been forthcoming. Issues of personal liberty and freedom of speech had taken precedent over enhanced security measures. The problem that we now face is balancing the issue of freedom with our desire to live in relative security.

Terrorism – Recent History

Terrorism is best thought of as a tactic used to gain political power, or for personal gain. Persons using terrorist tactics are motivated by a variety of goals. Within the confines of terrorists' designated goals, they use the maximum amount of force, brutality, and destruction that they can muster. While our current focus is on Islamic fundamentalists, we must not lose sight of the far right fundamentalists who often advocate the use of terrorist tools to accomplish their own goals. Timothy McVeigh's attack on the Muir Federal Building cannot be forgotten.

Terrorism is a ploy for attention. In today's "see-it-as-it-happens" environment, the terrorist has an advantage. Instant media coverage brings the terror directly into the homes of many potential victims. Terrorism, the tactic, is particularly attractive to those who lack traditional methods of recourse in addressing their perceived wrongs. The results are immediate unlike other traditional methods. With the capture of the Israeli Olympians in 1972 in Munich, Germany, a new era of terrorist news reporting began. News cameras were on hand for the entire spectacle and portrayed the scene to the world as events were unfurling. This on-the-spot media coverage has, in many cases, led to a situation in which terrorists notify the news agencies either immediately before or after a bombing or other such activity for the sole purpose of gaining worldwide attention.

A number of years ago, the U.S. Department of Justice noted, "Terrorism, often viewed as a means to a political goal, is becoming an end in itself" (U.S. Department of Justice, Law Enforcement Assistance Association, 1977, 3).

Terrorist Strategies

A prime motivator in training all terrorist organizations has been "indoctrination." Individuals associated with the group must believe both in the cause and in his or her own importance in securing the end result. A clear set of goals is established, and the education process establishes the priorities and leadership. The terrorist trains in all facets of marksmanship through the realization that both close fighting and sniper actions, tend to agitate the populace. Terrorists obtain their weaponry through varied means. The Irish Republican Army had, for many years, purchased their weapons through the international black market, while the Palestine Liberation Organization was supplied through Libya and other nations. As seen in the latest attack on the World Trade Center, terrorists also train in other areas including demolitions and other explosive devices. In addition, many terrorists are also familiar with biological and chemical weapons. Such weapons are used to terrorize the populace and cause an overreaction on the part of the public and government.

During the 1974 Hearing on Terrorism, conducted by the House Committee on Internal Security, several aspects of the strategy of terrorists emerged. Organized terrorists were taught to sabotage communications, assassinate officials, and plant bombs in order to intimidate the citizenry. They were taught to publicize every act of sabotage through every means available in order to show the government's inability to combat the terrorist activities. While the use of sporadic bombings and assassinations was highly effective, the committee noted that most terrorists found it inadvisable to kill a policeman due to the swift and violent retribution usually initiated by the policeman's comrades (Jenkins, 1972).

Carlos Marighella, author of the *Minimanual of the Urban Guerrilla* (1970), stresses the fear factor involved in terrorist attacks. Citizens eventually become afraid to leave their homes and will disassociate themselves from the police and the government in order to attain a relative sense of security from terrorist attacks.

There are many classic writings on the issues of guerrilla warfare and terrorism. Authors range from Mao Tse-tung, the "father of guerrilla warfare," to Jay Mallin (1974) and Douglas Fromkin (1975). In 1974, Dr. Frederick Hacker, reported to the U.S. Congress, House Committee on Internal Security, Hearing on Terrorism, that all terrorists fall into three basic motivational groups:

1. Criminal – motivated mainly by personal gain

2. Mentally Deranged – personal motivation, often accompanied by delusions or hallucinations

3. Political – motivation toward a real or imagined strategic goal

Islamic fundamentalists (i.e., Osama bin Laden) have political and often mentally deranged characteristics.

Fighting Terrorism

> "Wars in every period have independent forms and independent conditions, and, therefore, every period must have its independent theory of war."
>
> –Tse-tung, 1961, 49

The first major works on counter-terrorism appeared in the early 1960s. David Galula (1964) suggested that long-range planning is a necessary element in combating terrorism. Galula suggested an eight-step plan to counter established terrorists. In step one, Galula suggests that intelligence gathering, tactical operations, and propaganda operations are all necessary. McCuen (1966) agrees with Galula, advising, "A primary objective in the strategy of counter-terrorism must be use of police action to destroy or neutralize the revolutionary politico-administrative network" (32). Colonel William Neale (1973), however, notes, "Sheer force is not alone effective in combating terrorism. The ruling authority must identify and alleviate the genuine grievances of the population that are exploited by the terrorist. Those who feel wronged must be given legal opportunities to participate in political life."

During the mid-1970s, the Cabinet Committee to Combat Terrorism Working Group and the Law Enforcement Assistance Administration funded three studies:

1. The Mass Destruction Terrorism Study, 1975

2. The Near-Term Potential for Serious Acts of Terrorism Study, 1976

3. An Overview of Counter-Terrorism Technology, 1976

In addition to the above, the Department of Justice (DOJ) published a compilation of counter-terrorist technology. At that time, the DOJ recommended a gaming approach in training those who would be responsible for counter-terrorist actions. As early as 1977, Robert H. Kupperman, Chief Scientist, U.S. Arms Control and Disarmament Agency stated, "We are poorly prepared to deal with terrorism, especially the high-order acts" (Kupperman & Trent, 1979, 24).

While there has been no lack of research and speculation about terrorism, the United States has not developed a proactive anti-terrorist strategy. Our desire to retain maximum freedom has not allowed the restrictive measures that have been applied in other parts of the world. Those who have traveled in many European and Asian countries have seen some of the restrictions that might be necessary to reduce American vulnerability to terrorist attacks.

While the U.S. government has created a new cabinet-level position for the Office of Homeland Security, the first director, Tom Ridge, has a full plate. He must create a department from the ground up. While the United States has many different agencies gathering intelligence information, interagency cooperation has often failed to materialize on critical issues. Ridge's first task would appear to be coordination of existing intelligence. While this is a task that was supposed to be handled by the National Security Agency (NSA), there has been no explanation of how events from the 1995 disruption of a terrorist cell in Manila that detailed

plans to use passenger planes as flying bombs escaped authorities. Targets mentioned in the Philippine police reports listed the Pentagon, CIA headquarters, the Transamerica building in San Francisco, the Sears Tower in Chicago, and the World Trade Center in New York City.

There are more than 650,000 local and state law enforcement officers in the United States. Add to that another 11,500 FBI agents and agents from the CIA, NIS, and other intelligence agencies. The need for communication among these officers is critical but problematic.

The Need for a Predictive Model

There is a distinct need for a predictive model to assist the law enforcement officer responsible for the outcome of a given terrorist situation in determining the optimum course of action to follow. In this case, the predictive model is a working model with five independent variables and one dependent variable. The use of this model can be effective for law enforcement personnel when a given situation displays characteristics corresponding to variables contained within the model. As incidents increase and further data is gathered, the model can be expanded to include all permutations of the five independent variables.

The methodology utilized to gather the information to formulate the hypothetical model was divided into two major areas. The first area was a compilation of data available in published form. Books, periodicals, studies, and news reports were examined and analyzed for information and situations that pertain to the issue of terrorist activities.

The second means of collecting data was through the use of specific case data provided by agencies of the federal government in response to a request for this information. Case data was also provided by other agencies dealing with groups of terrorists falling into the confines of the five-stage Jenkins Model (Jenkins, 1972).

The use of document analysis in the formulation of a predictive model causes a certain amount of concern for the researchers. There is always the question of the veraciousness of the documents unless substantiating documentation can be found. The survivability and the obtainability of given information were also problems which could not be ignored by the researchers. For the purposes of the research, certain assumptions concerning the validity of document analysis were made. First and foremost, all documentation from government agencies certified as official was considered correct. Data contained in publications was considered accurate when it reflected information gained from official sources. Data gained through the use of news reports was considered accurate when verified through other sources. All terrorist activity from January 1970 through June 1982 was considered as long as the perpetrating organization fit into the Jenkins Model.

During the pilot study, which centered on document analysis, it became evident that certain variables appeared to influence the eventual outcome of short-term terrorist confrontations. These variables are the keystone of the study and should prove to be effective in formulating an effective counter-terrorist model.

Variables

The five variables that can be classified as independent variables are as follows:

1. Type of incident
2. Desired goals
3. Police ability to react
4. Media coverage
5. Police response

The dependent variable is the degree of success attained at the conclusion of the incident.

Type of Incident

The type of incident is of major importance in combating terrorism. Incidents studied indicated that three separate situations all tend to give a different "sense of urgency" to the responding law enforcement agency:

1. Direct hostage situations
2. Indirect hostage situations
3. Nonhostage situations

The direct hostage situation occurs when a terrorist or group of terrorists kidnaps or captures an individual or group of individuals in order to achieve the stated goals. Indirect hostage situations occur when terrorists use threats of violence, assassination, or injury to persons to attain their goals. Finally, a nonhostage situation occurs when a terrorist either captures property or threatens to destroy property to achieve an end. Each situation appears to have a different set of actions that terrorists will consider to be appropriate, those they will probably utilize to gain the desired result.

Desired Goals

The desired goals can be considered for the purpose of this study to be stated goals for the incident. The overall goals of the terrorist organization may conceivably be quite different from the short-range goals stated during a given situation. The desired goals reflect directly upon possible police actions. The goals of money, power, prisoner release, political action, and redress of past wrongs, might be easily negotiated under some circumstances and in some locations, but might not be legal in others. This research indicated that when the terrorist group selected a goal that was not only achievable but also grantable, the solution of the incident was usually more satisfactory to both sides; however, when the group selected a goal that was impossible to grant, violence usually ensued.

Police Ability to React

This variable was considered as a positive, negative, or unknown factor. In deciding the status of the police agency's ability to react, an analysis of the agency's level of training in a specific area, the ability of the leadership to command, the support received by the police from the constituency, and the historical evidence

to support a course of action being attempted must be conducted. This ability to react in a given situation will be a limiting factor in the selection of the optimum course of action to be taken. An agency incapable of using any of the available options would negate much of the benefit to be derived from this model.

Media Coverage

Media coverage has had a major impact on events since the advent of radio and television news coverage. This research indicates that there is a correlation between the motivation of terrorists and their desire for publicity. This variable will be evaluated based on the level of coverage of the incident as it is occurring. The incident will be recorded as receiving widespread coverage, little coverage, or no coverage. In certain instances, it has been shown that media coverage has proven to be beneficial to the law enforcement agency responsible for controlling the incident. These cases occur when terrorists do not want news coverage that will make their actions a matter of public record.

Police Response

The police response deals with the overall tactics utilized in the situation and is categorized in a range of five levels. The decisions that the law enforcement agency makes must revolve around the tactics of doing nothing, negotiating, agreeing to demands, not agreeing to demands, and/or using force. The overall strategy will, when combined with the other independent variables, react to form the dependent variable—demonstrated success. After the formulation of the predictive model, the law enforcement agency faced with an incident should be able to compare the independent variables in the present situation and analyze the best tactical options and responses to create an optimum degree of success.

Demonstrated Success

The dependent variable, the degree of demonstrated success, combines the measurement of two separate elements: (1) the capture of the terrorists and (2) the saving of life and property. When determining optimum solutions, the lives of the hostages will be more important than the capturing of the terrorists, but in each instance, the society must decide what the optimum result of a terrorist incident is.

Data Collection

Various federal law enforcement agencies agreed to participate in providing case studies. Some agencies forwarded case studies and general comments. Other agencies provided the names of commanders of counter-terrorist operations and requested that these commanders forward case studies.

Data collection was made both manually and by computer. Each incident was recorded and classified by its source of input and whether it had been substantiated by other documentation. While manual compilation was being accomplished, a computer comparison and analysis was made to assist in formulating a matrix to determine the validity of variables and in predicting the success probabilities of additional data as it was collected.

A database of 242 terrorist incidents was compiled for purposes of model development.

Data Analysis

Data analysis was performed through the use of the Statistical Package for Social Sciences (SPSS). Three basic questions were answered prior to the formulation of the model:

1. Are the independent variables truly independent?

2. Does police response matter in determining the dependent variable?

3. If the police response does not matter, which independent variable does determine the optimum success in the terrorist situation?

These questions as well as an additional question involving the use of each independent variable in relation to the dependent variable as a means of improving the predictive nature of the given incident were analyzed using SPSS. A cross-tabulation of type of incident and degree of demonstrated success shows that the relationship is significant. Further analysis of this relationship was conducted using asymmetric lambda, a statistical method that compares two variables and determines the improvement of predictability in a given target response. To quote Edwin S. Johnson (1981), asymmetric lambda "measures association, is used for proportional reduction of error in nominal-level variables, and is based on the prediction of categories of one variable when the other is known" (283). The use of this statistical method assists in formulating a predictive model. In this specific case, over 6% improvement in the ability to predict the degree of success is achieved when the type of incident is known.

The comparison of these two variables is important in that it enables the officer to predict the final outcome of a situation when only the type of incident is known. Analysis found that 19.5% of all direct hostage incidents resulted in a 100% degree of success; 58.1% resulted in the loss of the terrorists and the saving of all life and property; 9% resulted in the capture of the terrorists and the loss of some life and property; 2.4% resulted in the loss of the terrorists and the loss of some life and property; and 11% resulted in a total loss.

Indirect hostage situations and nonhostage situations showed a marked decrease in the percentage of the incidents in which all lives and property were saved. Sixty percent of the indirect hostage situations and 66.6% of the nonhostage situations resulted in the loss of some or all life and property compared to the 22.4% in the direct hostage situations.

Knowing the motivation of the terrorist failed to provide even a 2% improvement in the ability to predict the degree of success. This statistical insignificance may be attributed to the fact that 232 of the 242 cases studied were politically motivated. In effect, the "variable" was not a variable. For this reason, motivation was not used in the predictive model.

The relationship between desired goals and degree of success is significant. In analyzing cross-tabulation, when terrorists desired money, 235 of all incidents concluded with all lives and property being saved, but only 14.1% resulted in the capture of the terrorists. Terrorists seeking power were not apprehended in any of the cases studied, but 75% resulted in the loss of lives or property. Police officials had the greatest degree of success in capturing terrorists (38.9%) when the desired goal was the release of a prisoner. In this instance, they also had the highest rate of success in saving lives and property. When the terrorists sought political goals, there was a high incidence of the loss of life and property (33%), but a smaller percentage of cases in which the terrorists were caught (28%). Finally, in those instances in which the terrorist sought a redress of past wrongs, a high percentage of cases resulted in the loss of life and property (44.4%).

The relationship between the police ability to react and the degree of success is highly significant. Those agencies that had a positive ability to react captured the terrorists at a rate over three times greater than did those agencies that were not trained for a particular situation. Well-trained units saved all lives and property at a rate three and a half times greater (76.2% versus 21.1%) than did units that did not have a positive ability to react.

Agencies with a negative ability to react lost the terrorists and all lives and property at a rate over five times greater than did the better-trained agencies (47.4% versus 9.1%). Although this research considered an "unknown" category for agency response capability, the model discarded its use since the site commander would be capable of evaluating the level of training of responding personnel in actual situations.

The media coverage variable proved to have a significant relationship with degree of success; however, the data provided from the cross-tabulation did not appear to be of value to the police commander since the degree of coverage resulted in a similar percentage in the types of results. What is significant is that the percentage of the cases in which all was lost was about twice as high in situations in which there was no media coverage.

The most important comparison in the first series of analyses was the relationship between the actual police response and the degree of success. The asymmetric lambda shows a 15.8% improvement in the ability to predict the degree of success by selecting the appropriate police response.

An analysis of the matrix formed by a cross-tabulation of police response with the degree of success could lead the police commander to some significant conclusions. If the desired level of success is saving all lives and property, the optimum police response would be agreeing to demands (98.7%), followed by the use of force (73.5%), not agreeing to demands (58.9%), doing nothing (54.9%), and negotiating (38.1%).

If the capture of the terrorists were the desired result, the use of force (77.5%) would best accomplish the mission, followed by not agreeing to demand (30.7%), negotiating (22.2%), agreeing to demands (9.2%), and doing nothing (7.9%).

A Predictive Model

The actual predictive anti-terrorist model is composed of 12 separate matrixes with differing control factors. To use the model, it is necessary to first determine the control factor values. The variables in the matrix include the following:

- Type of incident (direct hostage or nonhostage)
- Desired goals of the terrorist (money, prisoner release, or political)
- Ability of the police to react (positive or negative)
- Media coverage (widespread, little coverage, or no coverage)

After selecting the appropriate values in the matrix, the police commander would analyze the degree of success for the optimum solution to the situation.

Prior to any terrorist incident, law enforcement and the appropriate political powers must decide on a definition of success for a given situation. In studying the 242 cases, success can be defined in terms of one of four outcomes:

1. All terrorists are either captured or killed; there is no loss of hostages and no property damage.

2. All hostage lives are saved, and no property is destroyed.

3. All terrorists are either killed or captured. Destruction of the terrorist is more important than saving the hostages.

4. Any outcome in which you do not lose everything is a success.

Each organization should predetermine and publish its concept of success.

Level 1

The first level of success is the most stringent and the most difficult to attain. This level involves the belief that 100% success must be achieved. This means that all terrorists would be either captured or killed, none of the hostages would be killed or injured, and no property would be destroyed. Injury to hostages and the destruction of property is only considered in this model when it occurs after the police have had a chance to respond, since injury and destruction occurring during the onset of the assault are not attributable to the decisions made by law enforcement officials. This degree of success occurred in only 19.4% of all tested occurrences.

Level 2

The second level of success occurs when all lives are saved and no property is destroyed. If the terrorists are killed or captured while saving the hostages, it is not defined as a failure. This level of success has been seen as appropriate in most cases. Unlike Level 1, this level comprises two separate but interrelated values in the degree of success. To save all life and property, the law enforcement agency can either attempt to gain a 100% resolution of the conflict, or it can attempt to affect the solution of losing the terrorists and saving life and property. This outcome

occurred in 128, or 52.9% of the cases. The possibility of success, when success is defined as the saving of life and property is 72.3%.

Level 3

The third level of success has proven to be the most effective in long-term deterrence. Success means that the terrorists are either killed or captured. At this level, the destruction of the terrorist force and not the safety of the hostages is the overriding concern. Many nations have opted for this solution and have used it successfully. Israel is the prime example of a nation that has refused to bargain with terrorists; it is dedicated to the wholesale destruction of terrorist elements. Success was attained at this level in 27.7% of the cases studied.

Level 4

The fourth level is viewed as totally pessimistic. The outcome is premised on the belief that terrorists will destroy the property involved and will kill hostages; therefore, any actions that save some hostages or kill or capture some terrorists are viewed as successful. This level can be further defined as the belief that any outcome in which you do not lose everything is a success. This level of success will be attained 88% of the time. The World Trade Center event would support this pessimistic view.

While there are numerous possible predictive models that can be constructed from this research, only three will be presented. The three models chosen present some of the most interesting ideas discovered in this research effort.

Predictive Model 1

Terrorists Desire Political Goals/Direct Hostage/Police Have Positive Response Capability/Widespread Media Coverage

	Degree of Success				
Police Response	**100% Success; Terrorists Captured; All Lives/ Property Saved**	**Lose Terrorists; Save Life/ Property**	**Capture Terrorists; Lose Some Life/ Property**	**Lose Terrorists; Lose Some Life/ Property**	**Lose All**
Do Nothing	0	60%	0	0	40%
Negotiate	20%	40%	0	20%	20%
Agree to Demands	0	83.3%	0	0	16.7%
Do Not Agree to Demands	25%	75%	0	0	0
Use Force	50%	12.5%	37.5%	0	0

Model 1 – Terrorists Desire Political Goals/Direct Hostage/Police Have Positive Response Capability/Widespread Media Coverage

This situation occurred in 14% of the evaluated cases. The most typical response in the cases reviewed was the use of force by the police. If the desired success option were the saving of life, the optimum response would be the use of force or agreeing to terrorists' demands. If the definition of success is set at Level 1, the model predicts 100% success (achieved in only 21.4% of the evaluated cases), then the use of force accounted for 62.5% of the successful cases, negotiating 20% and not agreeing to demands 25%. It should be noted that while doing nothing appears to be a reasonable option, a further analysis of this option reveals that while 60% of the time when this option was utilized, the saving of life occurred, the remaining 40% of the cases resulted in the loss of terrorists and all life.

Predictive Model 2

Terrorists Desire Political Goals/Direct Hostage/Police Have Positive Response Capability/Widespread Media Coverage Restricted

	Degree of Success				
Police Response	**100% Success; Terrorists Captured; All Lives/ Property Saved**	**Lose Terrorists; Save Life/ Property**	**Capture Terrorists; Lose Some Life/ Property**	**Lose Terrorists; Lose Some Life/ Property**	**Lose All**
Do Nothing	25%	50%	0	0	25%
Negotiate	50%	50%	0	0	0
Agree to Demands	0	100%	0	0	0
Do Not Agree to Demands	0	100%	0	0	0
Use Force	57.1%	42.9%	0	0	0

Model 2 – Terrorists Desire Political Goals/Direct Hostage/Police Have Positive Response Capability/Widespread Media Coverage Restricted

In this situation, 35% of the incidents studied were resolved with a 100% level of success at Level 1. The use of force accounted for 57.1% of all incidents in this category, followed by negotiating (50%) and doing nothing (25%). The level of success at the second level was attained 55% of the time, with the use of force accounting for 42.9% of these successes followed by doing nothing (50%), negotiating and agreeing to demands (100%), and not agreeing to demands (100%).

The big factor in the difference between Models 1 and 2 is the role of the media. When the role of the media was restricted, the rate of 100% success rose from 21.4% to 35%. The incidence of saving of all life increased from 71.4% to 90% with the limiting of media coverage.

It should be noted that the restriction of media coverage is not recommended in all models.

Predictive Model 3

Terrorists Desire Political Goals/Direct Hostage/Police Have a Positive Response Capability/No Media Coverage

	Degree of Success				
Police Response	**100% Success; Terrorists Captured; All Lives/ Property Saved**	**Lose Terrorists; Save Life/ Property**	**Capture Terrorists; Lose Some Life/ Property**	**Lose Terrorists; Lose Some Life/ Property**	**Lose All**
Do Nothing	0	100%	0	0	0
Negotiate	0	0	0	0	0
Agree to Demands	0	0	0	0	0
Do Not Agree to Demands	0	0	0	0	0
Use Force	100%	20%	20.5%	0	0

Model 3 – Terrorists Desire Political Goals/Direct Hostage/Police Have a Positive Response Capability/No Media Coverage

There is a major increase in the degree of success with the use of force (60%) as compared to other possible responses. Force was used in 100% of the situations that were resolved at a 100% success level, 57.2% of the cases in which all lives were saved, and 100% of the cases in which the terrorists were captured. Doing nothing resulted in the loss of terrorists and the saving of lives every time.

It is interesting to note when comparing Model 3 with Models 1 and 2, that the more restricted the media coverage, the greater the propensity of the police to use force. In Model 1, force was used 28.6% of the time. In Model 2, force was used 35% of the time. In this model, force was used 62.5% of the time.

While this might appear alarming, it should also be noted that the level of success also increases as the level of media coverage decreases when the optimum goal is Level 1 or the capture of terrorists. Level 1 success increases from 21.4% in Model 1 to 35% in Model 2 to 37.5% in Model 3.

If the goal is saving of all lives, the rate of success is relatively constant.

Conclusions

By using predictive models, police commanders may be able to determine, with a greatly improved percentage of accuracy, how possible responses would affect the outcome of the situation. Of particular note is the fact that if the desired level of success is either the capture of the terrorist and the saving of all lives or solely the capture of terrorists, data suggests that the greater degree to which the police can limit or curtail media coverage, the greater percentage of success they will achieve.

A major goal of this study was to produce benefits to law enforcement agencies faced with terrorist acts. The predictive model developed by the authors contains over 81% of the tested cases and attains a level of greater than 30% improvement in the ability to predict the outcome of a situation using a targeted response. This improvement is highly important when the number of hostage lives is taken into consideration.

Of particular significance are the conclusions concerning police response, use of force, and effect of media coverage on a hostage situation. Through a thorough analysis of the evaluated cases, it became obvious that as the level of media coverage decreased, the use of police force increased. Whether the police feared using force when under the scrutiny of widespread media coverage or they used force in a "spur of the moment" decision prior to the arrival of the media elements or they used force in those incidents the media felt to be too trivial to cover was not investigated.

The effect of media coverage on the final outcome was critical in that the presence of the media appeared to dissuade the police from using force as a viable option and that it aided the terrorist organization in spreading its word. While freedom of the press is guaranteed by the Constitution, unlimited media access to a tactical situation in which lives are in jeopardy is not a right.

Cutting terrorist groups from all or most outside publicity actually lessened the severity of the final outcome and appeared to shorten the length of time the hostages were held.

A total of 12 models was developed. Information on these models is available through Assets Protection Associates, Inc. 13601 North 1500th Road, Macomb, IL 61455.

Bibliography

Fromkin, D. (1975, July). The strategy of terrorism. *Foreign Affairs*.

Galula, D. (1964). *Counter-insurgency warfare: Theory and practice*. New York: Frederick A. Praeger.

Hacker, F. J. (1976). *Crusaders, criminals, crazies*. New York: Norton.

Jenkins, B. M. (1972). *An urban strategy for guerrillas and governments*. Santa Monica: Rand.

Johnson, E. S. (1981). *Research methods in criminology and criminal justice*. Englewood Cliffs, NJ: Prentice Hall.

Kupperman, R., and Trent, D. (1979). *Terrorism*. Stanford, CA: Hoover Institution Press.

Mallin, J. (1974, Fall). Terrorism in revolutionary warfare. *Strategic Review*.

Marighella, C. (1970). *Minimanual of the urban guerrilla.* Havanna: Tricontinental.

McCuen, J. J. (1966). *The art of counter-revolutionary war*. Harrisburg, PA: Stackpole Books.

Neale, W. D. (1973, August). Terror: Oldest weapon in the arsenal. *Army*, *23*, 10-17.

Tse-tung, M. (1961). *Guerrilla warfare* (S. B. Griffith, Trans.). New York: Praeger.

U.S. Congress, House Committee on Internal Security. (1974). *Terrorism: A staff study*. 93rd Congress. Washington DC: U.S. Government Printing Office.

U.S. Department of Justice, Law Enforcement Assistance Administration. (1977). *Facing tomorrow's terrorist incident today*. Washington, DC: U.S. Government Printing Office.

Bruce Heininger, PhD received his doctorate degree from Sam Houston University. He taught in the Law Enforcement and Justice Administration Department at Western Illinois University, serving as graduate coordinator. Bruce worked for the Houston Police Department, eventually moving to the Overland Park, Kansas Police Department where he served as their police planner until retiring in 2000.

Robert Fischer, PhD received his doctorate degree from Southern Illinois University. He taught in the Law Enforcement and Justice Administration Department at Western Illinois University also serving as department head. Fischer also worked as a police officer in Norman, Oklahoma. Over the past ten years, Dr. Fischer has served as the Director of the Illinois Law Enforcement Training and Standards Board's Executive Institute. In January 2002, Bob retired to work full time as the president of Assets Protection Associates, Inc.

Colonel Fred Berger (ret.) has served his country in a variety of assignments including work on counter-terrorism. Berger was involved in the War on Drugs working with the DEA. Fred is now the vice president of Business Plus, an information firm contracting with various law enforcement agencies.

Open Borders Policy and Countering Terrorism: The Experience of the European Union

Andrew Dalby

In the aftermath of the terrorist attacks on the U.S., there has been much soul searching as America struggles to come to terms with these atrocities and how they could have occurred. A couple of disturbing issues that have come to light after the identification of the suicide terrorists was how they had been free to travel within the U.S. (and other western countries) learning the skills necessary to execute these attacks. The terrorists were able to utilise the openness of a democratic society to their advantage and then strike at it. No law enforcement agency was looking for them prior to the attacks; they had entered the country with legal documentation and did nothing to draw undue attention. Equally disturbing was the disclosure of the laxness of the security attributed to domestic air travel. The United States' internal security apparatus was unprepared for an attack by international terrorists on home soil, despite two previous incidents (the 1993 World Trade Centre bombing and the thwarted Japanese Red Army bomb attack in New York in January 1988 by a suspicious state trooper on the New Jersey Turnpike). America is quick to learn from its mistakes, and the creation of the Office of Homeland Security will hopefully lead to greater coordination between the various law enforcement agencies in the United States responsible for countering terrorism.

The effective coordination of police and security forces is a key weapon in countering terrorism. The European Union (EU) Member States, many of which are seasoned veterans in dealing with both domestic and international terrorism, have slowly been learning this lesson over the past 30 years. Moreover, the majority of the EU Member States have dismantled the internal border controls of the Union to allow the realisation of Article 3 of the Treaty of Rome, commonly referred to as the "Four Freedoms": the free movement of goods, free movement of persons, freedom to provide services, and the free movement of capital throughout the Union.[1] Such freedoms necessitated an overhaul in the approach being taken towards law enforcement cooperation. These states would become vulnerable to criminals who could and would exploit the absence of border controls, able to run rings around an uncoordinated cooperative policy. This article focuses on the development and coordination of police cooperation in the EU to compensate for the removal of the internal borders and how this relates to cooperation in counter-terrorism. Its relevance lies in the parallels that can be drawn between a large federal society that has always practised the "Four Freedoms" and a region of sovereign states, that, until recently, regarded the control of borders as a matter of sovereign concern. Have the removal of these controls made Europe any more vulnerable to terrorism?

The Law Enforcement Cooperative Structures in Place Against Terrorism

Terrorism is most effectively tackled when done so from a united front. The water that the terrorist "fish" swims in becomes more inhospitable as the number of bolt holes and staging posts lessens. Despite the unique relationship enjoyed by the EU Member States, a united front against terrorism has not always been forthcoming. Too many examples of terrorist suspects simply being expelled rather than prosecuted or extradited exist. The Italian authorities simply released Abul Abbas, the orchestrator behind the hijacking of the Achilli Lauro in October 1985, despite U.S. demands for his extradition. France released the two killers of Izz al Din Qalaq, a prominent PLO "ambassador," in February 1986, after having served only half of their 15-year sentence.[2] Some countries have had constitutional problems that have prevented them from taking certain measures against terrorism (France, Ireland). In short, the political dimensions of terrorism are prone to sow disharmony on effective cooperation. Equally, the geopolitical makeup of Europe has served as a hindrance to police cooperation at various levels, typically through differences in cultural, lingual, and judicial systems. Despite these problems, cooperation against terrorism has been a continuing issue at the political, judicial, and police levels since the formation of the now defunct Trevi Group in 1976 in response to the Black September attack at the Munich Olympic Games in 1972.[3] Police cooperation has advanced the most within these three areas.

A number of instruments exist to facilitate police cooperation at both a general level and against terrorism specifically. These include Europol, Interpol, the Schengen Implementing Convention, the Police Working Group on Terrorism, the Terrorism Directory, and the numerous bilateral agreements that exist between individual forces. The main focus of this article is on the concept of open borders and how to police these against terrorism. In direct terms, the facilitation for cooperation of police activity over border areas is regulated through the Schengen Implementing Convention (1991) (save the UK, Ireland, and Denmark).

Terrorists and Borders

Terrorists have long exploited the existence of borders between sovereign states, utilising them to escape justice or as a staging post for launching attacks. Such borders are usually crossed illicitly, either clandestinely circumventing border patrols or posts, going through the "backdoor," or with the possession of forged or illegally obtained documents through the normal passenger travel stream. The likelihood of terrorists being apprehended crossing a border between democracies is questionable. Normally, it relies on the quality of the forged documents that they are using. For example, Greek authorities arrested and put on trial a suspected terrorist, Avraam Lesperoglou, an alleged member of Anti-State Struggle. Lesperoglou entered Athens Airport on an Air France Flight from Amsterdam in December 1999, having been on the run since 1982 and wanted for six cases of murder. He was arrested because he was travelling on a forged passport.[4] Terrorists typically have a sophisticated support structure behind them, and their possession of poor quality forgeries is rare indeed. Ahmed Ressam, the terrorist who was arrested by a suspicious customs inspector, while attempting to enter the U.S. from Canada on a ferry in December 1999 with bomb making equipment, was found to be in possession of a legitimate Canadian passport, obtained by using a false name. It is suspected that Ressam is connected to the

Algerian Armed Islamic Group (GIA), and possibly obtained this passport with the help of Karim Said Atmani, a reputed GIA document forger with whom he shared an apartment in Montreal. This case also demonstrates an increasingly employed strategy among terrorists: entering the target country through a friendly neighbour, thereby lessening suspicion as against say, entering the country on a flight from the Middle East. Equally, border controls are more lax with such a country, as opposed to entering the U.S. from Mexico for example, where a steady stream of illegal immigration only strengthens security. A classic historical example of a foreign foe exploiting such a situation is Germany in both world wars; its army avoided France's heavily fortified Maginot Line by attacking through Belgium.

Passing through "unguarded" back doors is an option for terrorists, especially if they have weaponry or ordnance to smuggle in or feel that they may be being watched. It is obviously much harder to police such incursions without significant expense and diversion of resources from other law enforcement programmes, so luck and deterrence must be heavily relied upon here. This has been a much more common strategy within Europe than the U.S. for purely geographic reasons. The border between the Irish Republic and the North is frequently a crossing point for Republican terrorists. South Armagh, nicknamed "Bandit Country," is a dangerous place for the security forces' patrols. The Spanish Basque/French border also experiences Basque Fatherland and Liberty (ETA) members moving secretively back and forth. Interestingly enough, despite the removal of border controls throughout most of continental Europe, ETA members continue to traverse the border by way of long hikes through the mountains. In this case, such a mentality is probably derived from the desire to continue to install a quasi-military outlook on ETA's membership, thereby retaining the perception of being a guerrilla force rather than terrorists.[5]

Alex Schmid comments that "(p)rofessional European terrorists . . . are not impeded by present borders. They have crossed borders in Europe for a long time, and for them, the changes introduced at the end of 1992 will not make much difference."[6] The examples of incursions above are only a couple. Border controls did not stop Provisional Irish Republican Army (PIRA) Active Service Units (ASUs) targeting British Army personnel in continental Europe during the 1980s, nor stop GAL (Grupa Antiterrorista de Liberacion) Death Squads entering France from Spain to eliminate suspected ETA members.

While there is sufficient evidence demonstrating the case against the effectiveness of border controls against terrorists, those who do favour them point to the fact that many arrests occur at the border. The reality though is that the border check represents a convenient location to make an arrest; arrests are usually made thanks to advance warning or surveillance. One advantage is that if the intelligence regarding the terrorist comes from an informer, a "random" check at the border may mask this breach in the terror organisation's security. A significant case in point of border controls working effectively against terrorism is the confrontation of a PIRA ASU by Special Air Service (SAS) troopers in Gibraltar in March of 1988. Spanish immigration officials pass on all details of Irish passports to Madrid's Servicios de Información's Euro-terrorism office. They in turn check the details with MI5 in London (prior to October 1992, the police Special Branch dealt with Republican terrorist intelligence). Such checks enabled the British security forces to

detect the arrival of the ASU in Gibraltar and activate counter-measures against it.[7] This particular incident was detected though because Gibraltar is a small island. The ASU would have had to come across through conventional channels, as any other way would most likely draw unwanted suspicion (e.g., bribing a fishing boat to drop them on the coastline).

In dealing with Irish terrorism, the view of British police officers has always followed the line that . . .

> [I]t would be totally irresponsible for the British authorities and the Irish . . . to abandon checkpoints, road blocks, and other devices for assisting security against terrorism . . . Open borders are simply not a sensible option for either the British or Irish Governments.[8]

The security measures of the Irish borders can perhaps be seen as an exception to the argument that border controls do not stop terrorists. Of course, terrorists cross the border between the Republic and the North, but the border has been an open one due to a common travel area agreement between the UK and the Republic well before their entry into the European Union (EEC) in 1972. The sole purpose of the security measures and structures that exist here has been to counter terrorism. Take away the threat and the guard towers, and checkpoints are no longer required. The dismantling of some of this security apparatus as the peace process continues has proved this. In addition, this border is a specific traffic corridor for a large number of terrorists and geopolitically epitomises "the troubles." It is policed because of this. In the case of ETA, France and Spain re-established surveillance along their common border in the Basque region in August 2000, after renewed ETA violence. Only borders that fall into this specific category are worth the effort of enforcing security apparatus along them. Thus, even though some terrorists hostile to the U.S. have entered into the country through Canada and may continue to do so, this cannot justify in security terms, let alone economic, fiscal, or geographic terms, the introduction of such counter-terrorism measures as have existed along the Irish border.

Current border controls should be considered a precarious defence against terrorism. Within the EU, Member States have devised a new structure to compensate for their missing border controls through a regulation of police cooperation along and across borders and the installation of a computerised database. The Schengen Implementing Convention (1991) was designed to implement the Schengen Agreement (1985) fashioning it into reality by dealing with the practicalities of Member States operating under the "Four Freedoms." Its ultimate success cannot be measured yet, as having entered into EU law through its incorporation by the Treaty of Amsterdam (1996), "the Schengen acquis," as it has become known, has developed into a vast behemoth of legislation.[9] Its full absorption into EU and Member State law will not be a smooth process. Additionally, the acquis is bedevilled by questions of accountability. The complexity of its machinery and its status as a body of international law make it difficult to achieve adequate accountability at the national level.[10] While incorporation into the EU has generated a greater element of openness and accountability because of the European Parliament's ability to scrutinise aspects of Schengen, security concerns are still under intergovernmental jurisdiction.

In security terms, the Implementing Convention's emphasis has been to shift the focus of security away from internal borders to that of a heavily sentinel-orientated one at the external borders. Border checkpoints are linked to the Schengen Information Service (SIS), a vast computer database capable of holding information on up to eight million people and seven million objects.[11] The service is provided through the National SIS database (in turn linked to the central database), helping to monitor the movement of undesirables and fugitives attempting to cross the EU border. Rapid electronic transmission of photos and fingerprints, ballistic images, DNA profiles (the EU is to create an international DNA database), and direct links with diplomatic missions outside the EU allowing the "exchange of data on the issuing of visas" are some of the services offered by SISNET, which functions as a single input and output data exchange network.[12]

The SIS database is not actually permitted to contain criminal intelligence (due to the need to achieve a balance between a regional membership and their data protection legislation); rather, it is limited to defined categories (Title VI, Chapter II, Articles 93-101): real and assumed names, physical distinguishing marks, initial letter of second forename, date and place of birth, sex, nationality, indication that the person is armed or violent, reason for the report, and action to be taken. The types of persons who are subject to SIS reports are as follows:

- Persons to be arrested for extradition purposes, on the basis of an arrest warrant or a sentence
- Aliens who are reported for the purpose of being refused entry on the basis of a national decision
- Persons having disappeared or persons who, in the interest of their own security, need to be placed in a secure place
- Persons required to be located for the purpose of judicial proceedings, because for example, they are witnesses who have to appear before a judicial authority
- Persons required to be subject to discreet surveillance or specific checks for crime prevention purposes

Individuals who have no reason to appear on the SIS watch list will not be on it.[13] Terrorist suspects by definition tend to fall among either the first or final category; however, in the case of the last category, such suspects would and could not be detained by border guards: They have done nothing wrong. Their passing would simply be logged into the SIS database. This definition also suggests indigenous terrorists or those already residing in an EU state but not those outside. This blindside, if it can be called that, is negotiated by Article 99, which allows information to be included in the SIS but *only* if a state's security apparatus is already suspicious of an individual to the point that he or she represents a "threat to public safety." The conditions for this are as follows:

- There are real indications to suggest that the person concerned intends to commit or is committing numerous and extremely serious offences.

- An overall evaluation of the person concerned, in particular on the basis of offences committed hitherto, gives reason to suppose that he or she will commit extremely serious offences in the future.

Additionally, Article 99(3) permits the state security forces to request that a report, beyond that permitted for SIS information on individuals, be included in the SIS if the said individual represents a "serious threat to internal and external security." This is subject to the authorities' possession of "concrete evidence" and whether other contracting parties are contacted beforehand. This is much more unambiguous in that it is primarily aimed at terrorists, without getting mired in actual definitions of terrorism, something which even the EU Member States have not always been totally unanimous on. Once again though, this is only of any real use if the authorities know who to look for; otherwise, this information would only be triggered if a terrorist were to enter the EU legitimately, and this is rare indeed.[14] As the events of September 11 demonstrate, such measures are of no use if "unknowns" are used.

The Implementing Convention does contain a derogation clause. Article 2(2) allows border controls to be reinstated at anytime if "public policy or national security so require" for a "limited period." France, for example, made use of this in April 1993 to prevent "illegal immigration and the spread of Islamic fundamentalism"[15] and again following a series of GIA bombings in Paris during the summer of 1995. From what has already been discussed vis-à-vis the porosity of borders, it is debatable how effective such measures against GIA terrorism would be.

In addition, France has continued to maintain border controls along its Belgian and Luxembourg borders as the French government says that they act as transit countries for drugs leaving the Netherlands.[16] With Germany, however, it reached an agreement to remove these controls in April 1996 and instead maintain "mobile border controls" (Schengen calls for the removal of permanent controls.). The Belgian Interior Minister, Johan Vande Lanotte, said that France's border checks were not working on the common border with his country and that "mobile" or "surprise" checks were much more efficient than static control points.[17] The French European Affairs Minister, Michel Barnier, said that these "could be more effective than fixed controls."[18] These "mobile frontiers" were introduced at a meeting of the Schengen Executive Committee in October 1995 after a proposal by Germany to recognise their creation under bilateral agreements between Schengen members, and such a network of agreements now exists within the Union. It should be noted that such "mobile frontiers" do not exist on the border itself, but on either side of it. The effectiveness of these measures is comparable to that of police patrols in cities, be they on foot or in vehicles. Of course, it would most likely come down to luck for such a patrol to catch a terrorist crossing the border. More importantly is that mobile patrols can be used in the same way that terrorists are often arrested at frontier checks as a "chance" encounter to hide the role of informants.

In analysing the effectiveness of the SIS, one can conclude without too much difficulty that it does not make much difference in preventing the comings and goings of terrorists than traditional border checks did. Geography is always going to be a detrimental factor in this area. The exceptions of course being islands whose points of entry are specific ports and airports, which are much easier to police.[19] The introduction of mobile patrols and the sophisticated information

transfer of SISNET are welcome additions to law enforcement measures that may yet produce results in apprehending terrorists; however, the fact of the matter is that the Implementing Convention is a tool primarily aimed at stopping illegal immigration and smuggling of goods. The former having become the primary security concern of the EU in recent years, the SIS database is very useful, holding details of the legion of illegal asylum seekers who have attempted to enter the EU once before.

The Implementing Convention's other area of facilitating police cooperation lies in its regulatory powers. By providing a structure that regulates cross-border police behaviour on a pan-European basis, law enforcement cooperation in this area is simplified in the sense that there is only one "rulebook" to follow. This can be supplemented by additional cooperation agreements at the bilateral level as the Implementing Convention allows for this. Areas covered by the Convention include the exchange of liaison officers (Article 47), information exchange on a requested basis (Article 39), and information exchange "without being asked" to prevent "future crime and offences against or threats to public policy and security" (Article 46). This goes beyond the traditional "reactive" style of cooperation, introducing instead an approach in which initiative is encouraged, and a cooperative spirit is introduced. The issue of "hot pursuit" across a border (Article 41) remains a controversial one, challenging the old concepts of sovereignty. How far a police officer may engage the pursuit across a border is governed by bilateral agreements between the individual states. Belgium and the Netherlands, for example, have followed Article 27 of the Benelux Agreement in this regard (10 km), while Germany has allowed unfettered access in pursuit distance and arrest powers (it is the only signatory to permit this). Firearms though (where carried) may only be deployed by officers in the event of self-defence. Arrests, though, may not be made (save in Germany) by officers who have crossed the border. They may only detain the fugitive and await arresting officers from that state (whom they must contact upon crossing the border), after which extradition procedures must be enacted.[20] Also useful is the concept of cross-border observation of suspects (Article 40), conferring the right of police and customs officers to cross a border to continue observation that began on their own territory. In the event of an emergency, prior authorisation is not required.

The topics discussed above demonstrate physical types of cooperation between police officers of different countries, leading to the development of contacts between these forces. This should not be overstated, as much of the contact will be between police officers who are based in the border areas and will often have already developed contacts with their opposites on the other side. One cannot, however, understate the significance of Article 46. It has the potential to foster strong links between police forces throughout Europe. As for how effective such measures are against terrorism, one should place them in the context that a terrorist is also a criminal and should be treated as such. It is curious to note, however, that terrorism is not listed as one of the 12 crimes necessary to warrant cross-border intervention. For that matter, no mention is made of it in any context in neither the Convention nor Schengen Agreement. The explanation as to why has already been made above; the point is to emphasize that terrorism is treated as a normal crime in the context of Schengen. The list contains among it the crimes of murder, assassination, kidnapping and hostage taking, and/or the use of explosives. A wanted terrorist is usually guilty of at least one of these, and is thus placed in that category(s).

Coordinating Police Efforts Against Terrorism

If Schengen's security measures are comparable to a cumbersome giant that the terrorist may sneak past, then this is not something that has been lost on the governments of the EU. The compensatory measures on open borders are not simply a case of merely strengthening the external frontiers. The "Four Freedoms" facilitate greater movement throughout Europe, and this in turn means that more and more police forces will find EU and non-EU nationals transgressing on their soil. Equally, the collapse of the Soviet Empire has augmented the criminal fraternity of organised crime, much of which lies on the eastern border of the affluent EU. To meet these challenges, greater coordination in police cooperation is required. Europol has been EU Member States' other response to this.

Europol

Established in 1995 and based in The Hague, Europol exists in a support capacity to aid "two or more Member States . . . in such a way as to require a common approach . . . owing to the scale, significance, and consequence of the offences concerned" (Article 2.1, Europol Convention). Its main attributes lie in its ability not only as a vessel for information exchange but that it has the resources to process raw data into analysed intelligence.[21] Other principle duties under Article 3 include the following:

- To notify the competent authorities of the Member States without delay via the national units of information concerning them and any connections identified between criminal offences
- To aid investigations in the Member States by forwarding all relevant information to the national units
- To maintain a computerised system of collected information containing data

Unlike the SIS, Europol's computerised database can include criminal intelligence, but perhaps more significantly and especially as far as counter-terrorism is concerned, this may include "persons who there are serious grounds for believing will commit criminal offences" (Article 8.2). Known terrorist suspects would of course fall under this category.

A significant development for Europol has been the Amsterdam Treaty through which it was agreed to augment its powers, including the granting of "operative powers" to the fledgling police structure. This "operative" mandate is totally distinct from "operational" powers to which countries such as France and Britain are inherently hostile. Rather, these "operative" powers will allow Europol employees to accompany national police forces in joint operations in an advisory support role. Amsterdam also allows Europol to request information from national police authorities and if necessary to conduct investigations on their behalf. The importance of the Third Pillar to the Member States became apparent when in October 1999, a two-day summit at Tampere was devoted to this issue, and discussion was given to the new powers and remits provided by Amsterdam and how best to implement them.

Prior to the removal of Europe's border controls, counter-terrorism cooperation was addressed primarily through two groups: (1) Trevi and (2) the Police Working Group on Terrorism (PWGOT). Both operate(d) as informal ad hoc groups. Established in 1976, Trevi operated at the intergovernmental level, composed of interior and justice ministers, police, and intelligence officers of the EU Member States to promote ground level cooperation. Initially concerned with terrorist matters, its success caused it to grow into other areas of policing, compartmentalising it into four different working groups. By including participants at the ministerial level, it gave it an element of political clout, a useful string to the bow when dealing with terrorism. As terrorist incidents such as the murder of Aldo Moro (1978) and Sir Richard Dykes (1979) continued, however, there was a feeling among police officers that greater work could be achieved in an even more informal atmosphere, which was subject neither to direct political supervision nor a bureaucracy. Awareness was growing that Trevi was not sufficient in itself to provide the necessary means to facilitate the cooperation required against terrorism; rather, there was a desire to create a "needs-orientated forum" which would cater to the requirements of police agencies.[22] The PWGOT is best described as an informal "alliance of Western European Special Branches, similar police agencies, or security services with the police powers who hold national, executive anti-terrorist responsibilities within their own countries."[23] It is comprised of members from the 15 EU states and Norway; they meet every six months in a different European capital.[24]

In both cases, a secure telecommunications system to transfer data has been employed. The PWGOT's new coded facsimile system which had been in operation since 1988, allowing regular, rapid, and secure information transfer was so successful that Trevi decided to apply it to its own network. Security in the transfer and handling of information is something that cannot be understated in terms of fostering cooperation in matters of terrorism. Such extremely sensitive information would simply not be transferred if it were felt that the communications system was insecure. Equally, the issue of trust plays a paramount role in cooperation in this area. The world of counter-terrorist officers is a small one; individuals are likely to become aware of and know their opposite numbers throughout the EU. A European Liaison Officer[25] of the Metropolitan Police Special Branch illustrates this point:

> I cannot stress too much the importance of the police-working group across the whole field of terrorism in Western Europe, including Northern Ireland. We know these people; they come here to the Yard when they happen to be in London. We make contact with them when we go abroad, regardless of what we are going for. It has become a solid group of working colleagues. We trust each other implicitly and pass information on to each other without question.[26]

Trust is undoubtedly a key factor in sharing this type of information, and the PWGOT has been functioning since 1979, providing it with an established trust among its participants. Europol is a fledgling by comparison, and a formal regulated institution to boot. How does it accommodate itself to obtaining the trust necessary from the Member States police and security agencies to function effectively?

Europol and Its Counter-Terrorist Mandate

Europol's remit in countering terrorism came into effect on July 1, 1999. This is undertaken through Europol's counter-terrorism unit, which had been in a preparatory phase since June 1998. The explanation behind such a delay in incorporating one of Europe's cornerstones of cooperation in internal security matters lay between the reservations of most Member States to this, and opposition in particular from Britain, Denmark, and France.[27] This latter group felt that to include a counter-terrorist role would severely hamper Europol in practical terms because of the political connotations and definitions associated with terrorism and that the existing PWGOT could do the job equally well, if not better. Disagreeing with this view were Spain and Greece, who were concerned about the ongoing terrorist campaigns in their own countries, pointing out that Article K.1(9) of the Treaty on European Union (TEU) did make reference to a counter-terrorist role for Europol, and that its eventual inclusion had been agreed in principle at the November 1993 meeting of the Justice and Home Affairs (JHA) Council. That most Member States expressed reservations, was countered by their general indifference to the debate, allowing the continuous pressurisation from these two governments to permit the tabling of a Spanish motion at the May meeting of the JHA Council on the draft Europol Convention that asked for terrorism to be provisionally inserted into the June 1994 draft. Here the German presidency adopted a gradualist approach, addressing nuclear crime in the initial brief with other aspects of terrorism to be included later. Spain remained unimpressed with this arrangement—its indigenous terror group, ETA, being national separatists, have little use for employing such a weapon—and continued to press for clarification on counter-terrorist cooperation. In light of this, the subsequent French presidency (1995) put forward a classic compromise: Europol's mandate would be extended to general counter-terrorist matters two years after the signing of the Convention. This delay would serve as a "warming up period in less stormy waters,"[28] as well as provide a breathing space to allow Member States to prepare for this incorporation. The proposal also suggested that Europol have access only to information held by police forces and not that of intelligence services. The purpose of this last point was to alleviate concerns of creating a Europol of two differing networks. Data protection concerns demand that all data presented to Europol is gathered legally; even then, the data must be sifted on an individual basis to ensure that it will not infringe upon a Member State's laws. This also removes another would-be sticking point.

On the issue of maintaining trust, Europol, as an institution, has adopted a dual strategy of ensuring that a high level of security is maintained through advanced telecommunications and through the physical measures taken on the protection of the building. Additionally, the counter-terrorism unit is self-contained in terms of security and operates under the highest security clearance within the building. The second approach focuses on the strategy adopted for Europol investigations. Such investigations focus their analysis from the information provided by individual Member States, but that information cannot be disclosed to any other investigation concurrently undergoing within Europol, even if it might be relevant to that investigation. To provide an illustration of this, suppose an investigation by the Organised Crime Unit contains information provided by France, Italy, and the UK (A), and an investigation by the Terrorism Unit contains information provided Spain, France, and Germany (B). Both investigations contain

information given by different groups of Member States, and because of this, there can be no cross-contamination of evidence, even if it were suspected that there was a common link between the two cases. The outcome of the investigation is a product for the agencies of A only (and vice versa). The single exception to this is that of the unit dealing with financial crime which may pass on any relevant information to a terrorist investigation, due to the methods used to fund terrorist groups. This rule does not easily make for common sense, but there is a necessary logic behind it. By maintaining these strict parameters, Member States and their law enforcement agencies can be assured that they are maintaining an element of control over the often sensitive information which they input into Europol. Europol currently has the membership of 15 sovereign countries; none of these members are going to throw sensitive security-orientated information into a common pot. It need not always be a case of how much you trust your neighbours either; often it is just a case of a "need to know" basis. This is the price that had to be paid to overcome the initial scepticism from police agencies when Europol was first established. Agencies need to feel a sense of trust and confidence in it, without which its role in countering terrorism would be null and void.

The Significance of Europol's Role in Counter-Terrorism

The service offered by Europol is centred on a new approach in tackling terrorism cooperatively. Europol enables, for the first time, the placing of all areas of European police cooperation concerned with serious crime under one roof. Prior to this task-specific ad hoc, working groups dealt with these concerns. No over-arching control structure for such groups or generalised cooperation existed. Even the Trevi Group, the most organised and all-encompassing of all these groups, was seen, due to its informal structure, as something closer to an "old boys network" or "club."[29] The maintenance of these separate cooperative groupings produces a nonsystemic approach, one that is incapable of harnessing the full potential of growing cooperative links that are developing between law enforcement bodies. Cross-pollination does occur between counter-terrorist and other policing groups, typically through the passing of nonsensitive intelligence and the exchange of liaison officers. This degree of inter-level cooperation, however, does not lend itself to the necessary compensatory measures required to provide a system that does not duplicate work or refrain from passing on useful information (mostly unknowingly). Europol does not remove these negative points absolutely, but it is a significant move in the right direction. The centralisation of these functions under one institution prevents fragmentation and the establishment of protectionist fiefdoms in this area, which are harmful to the spirit of cooperation. A more regulated structure allows intelligence to be stored in central databanks, which can be readily and rapidly accessed by Europol's liaison officers in response to requests from police and customs authorities.

In direct terms, Europol offers a greater multilateral approach to tackling terrorism. The subsequent arrests after the events of September 11 demonstrate the global scale of the al Queda network, a classic example of the terrorism/hydra analogy. Uprooting the network in one country is no longer sufficient protection; it has become an international problem. Europol, operating on a pan-European scale, is a move in the right direction. Its novel approach to conducting analysis allows for a greater chance of discovering hidden connections and establishing these within the construction of a multi-lateral picture. This is vitally important as it increases

the likelihood of intercepting a criminal activity before it is executed, all the more so now that there exists a well-entrenched terror group that has demonstrated its willingness to employ mass casualty terrorism and is in possession of radioactive materials.

The Terrorism Directory

Established by the Council of Ministers in October 1996, the terrorism directory is designed to facilitate cooperation in tackling terrorism through creating a directory of skills and expertise available to each Member State. Originally maintained by the holder of the EU presidency, it was later decided that greater continuity lay in having one keeper. Europol was chosen for this. The directory in itself is not a significant tool, but its functioning lies purely in practical terms. Consider the case of the kindergarten siege in Luxembourg in June 2000. It could not be certain whether or not the authorities were dealing with a terrorist, and Luxembourg being so small, does not maintain any specialised police forces to deal with this type of situation. By consulting the directory, it was possible to obtain a negotiating team rapidly, including a member who could speak the hostage-taker's language (he was of Tunisian origin).

Putting the Pieces Together

A useful addition to the pooled information and cooperation that occurs against terrorism is the existence of a bomb data centre. Member States can input data regarding terrorist bombs, the type of explosive used, the wiring, etc. By comparing information within the database with a new Improvised Explosive Device (IED) discovered by the police, it becomes possible to detect a signature pattern. This can be especially useful in tracking down those responsible as it allows lines to be drawn with previous terrorist incidents.

Interestingly, such a system does not extend to ballistic analysis. While SISNET plans to introduce the electronic transfer of ballistic images, this does not seem to extend to a database. Logic suggests though that it is only a matter of time before such a database is introduced. With no border controls, a criminal who is travelling across Europe has little need to dispose of his or her weapon. Many contract killers use a favourite weapon; it is after all a tool of their trade.[30] To illustrate this is the case of a contract killer arrested by French police for a murder in Marseilles. It was only discovered by accident that he had also been responsible for a "hit" in Spain and Italy. The existence of such a database would have allowed the investigating police forces to cross-reference their information and could have led to an arrest sooner.[31]

Conclusions

Democratic societies are as vulnerable to terrorists as any other society. Their weakness lies in their openness, but their strength rests in the stability of the state and their willingness to work with other like-minded states. Terrorism is certainly a thorn in the side of the democratic state, and like a thorn, the pain and irritation it causes far outweighs the damage that it can do.[32] The measures we take against terrorism must mirror the latter truth and not that of the former perception. When the European Member States began to address the compensatory security

measures necessary for facilitating the "Four Freedoms," the threat of terrorism was a diminishing one. Consequently, it took some political maneuvering by the likes of Spain and Greece to incorporate it into the package. What exists is an enhanced series of tripwires covering the EU rather than an expensive augmented external border, which in truth is only ever temporary on the eastern border as the EU is an organic expansionist structure. The year 2004 is the date set for the next round of accession. Alertness will be increased by the fact that police agencies will be able to pass on not just the usual type of information about terrorists, but the little pieces of seemingly unconnected information, which when filtered through Europol's analysis, has the potential of providing information greater than the sum of its parts when filtered through Europol's analysis. This is how terrorists will be caught, by the effective coordination of police agencies' efforts on a transnational scale. The terrorist hydra must be engaged by law enforcement acting as a hydra also.

Europe's model is by no means perfect, but it is one that has not sought to increase police powers. Rather, it is learning to pool through cooperation where necessary. After the September 11 attacks, the EU Member States have not sought as a whole to increase police powers. Instead, they have decided to begin to implement existing decisions as part of the Tampere Summit. Schengen was not temporally suspended throughout the EU in the wake of these atrocities. This decision speaks volumes; it was a statement that this is a problem that cannot and must not be tackled alone. What we may be beginning to see in tackling terrorism is final recognition of the "one for all, and all for one" spirit and approach.

Endnotes

[1] The United Kingdom, Ireland, and Denmark have chosen to retain their border controls.

[2] This type of behavior was especially common during the 1970s before any cohesive structure existed among the European states for dealing with terrorism.

[3] An informal body operating at an intergovernmental level, composed of interior and justice ministers and police and intelligence officers of EU Member States to promote ground level cooperation. Initially concerned with terrorist matters, it grew to include other areas of policing. Trevi was officially dissolved at the end of 1992 to make way for Europol, the European Police Office.

[4] Suspected terrorist arrested, jailed for forgery. (1999, December 27). *Athens News Agency: Daily News Bulletin in English*. Lesperoglou was imprisoned for three and a half years on forgery charges. It could not be proven that he was a terrorist.

[5] Organised Crime and Terrorism Conference, University of St. Andrews, June 2001.

[6] Schmid, A. P. (1993). Terrorism and democracy. In A. P. Schmid & R. D. Crelinsten (Eds.), *Western responses to terrorism* (p. 18). Wiltshire: Frank Cass.

[7] Adams, J., Morgan, R., and Bambridge, A. (1988). *Ambush: The war between the SAS and the IRA*. London: Pan Books, p. 145.

[8] The views of the Scottish Police Federation in *The House of Commons Home Affairs Select Committee on Practical Police Cooperation in the EU (1989-1990)*, (HCHASCR 363-I) (Stationary Office), p. 55.

[9] The House of Lords Select Committee on European Communities 21st Report (17 March 1998) stated the government's problems in obtaining a full definite list or version of the acquis for both Houses. This is due to the parts of the acquis having been superseded by EC treaty, while some, for example, no longer relate to circumstance. Consequently, there was an unanticipated delay in the Lords' scrutiny of it. An understanding of the size of the acquis is demonstrable by the fact that one part of it that relates to "Decisions and declarations adopted by the Executive Committee established by the 1990 Implementing Committee, as well as acts adopted for the Convention by the organs upon which the Executive Committee has confirmed decision making powers" runs to some 3,000 pages.

[10] House of Lords, 31st Report, paragraph 45.

[11] Benyon, J., Turnbull, L., Willis, A., & Woodward, R. (1993). *Police cooperation in Europe: An investigation*. Leicester: University of Leicester, UK, p. 237.

[12] SISNET was scheduled to come into effect in mid-2001, simplifying a system that previously employed multiple input and output networks. Incorporated within this is the old Supplementary Information Request at the National Entry (SIRENE) system, designed to process enquiries as rapidly as possible (especially useful if the length of detention that a suspect may be held before being charged or released is 24 hours). SIRENE was staffed with not only the representatives of the national police authorities, but also customs officials and crucially, legal experts. The latter's main function being not only to answer enquiries regarding the judicial system, but also to serve as a safeguard against a reply to a request which is technically illegal due to judicial ignorance. This is important because the onus is on the requesting country to examine whether a measure such as covert surveillance is legally permissible or not under the law of the requested state prior to making the request unlike Interpol, where information is only released once national legal conditions have been met. In short, it prevents a prosecution case or extradition hearing being thrown out or falling apart because procedures were incorrectly followed.

[13] Although, mistakes have been made. One particular documented case concerns Belgian police boarding a train in November 1992, picking out two Welsh football fans and then detaining and deporting one of them. Their names had been supplied to the Belgian police by the UK's National Criminal Intelligence Service, which in turn received their names from the Luxembourg authorities, who had incorrectly claimed that the two had "caused disorder" during a security check carried out in 1990. Even then, it took a six-year campaign to get their names removed from these files [Peers, S. (2000). *EU justice and home affairs law*. Essex: Pearson Education Ltd., p. 188.]

[14] It does leave open the possibility that an individual's answers to an officer might arouse suspicion, as they did in the case of Ahmed Ressam, in which case, entering the individual's physical characteristics into the database might produce a match.

[15] Bulletin: Monitoring the State and Civil Liberties in the European Union. *Statewatch*, *3*(3). (1993). p. 1.

[16] The Netherlands maintains a liberal approach to drugs in its domestic policy.

[17] Bulletin: Monitoring the State and Civil Liberties in the European Union. *Statewatch*, *6*(3). (1996). p. 19.

[18] Bulletin: Monitoring the State and Civil Liberties in the European Union. *Statewatch*, *5*(6). (1995). pp. 5-6.

[19] For this reason, the UK has not signed up to the Schengen acquis which would mean the removal of its internal borders. It has however signed up to the SIS. Ireland and Denmark have similar policies.

[20] Spain and Italy have entered into a common judicial area, whereby extradition has been converted into an administrative transfer. This allows that the surrender of the fugitive can only be *denied* if the documentation provided by the requesting state is incomplete or unsatisfactory or if the fugitive has been accorded immunity in the requested state. Portugal and France were also approached by these countries on this matter, but while demurring, they remain interested in the concept. It is anticipated that with time this type of system will encompass much of the EU Member States. In terms of terrorism, the EU plans to install European arrest warrants by December 2001, which will mean doing away with the internal extradition system.

[21] Its analysts are trained not only to work with the data that they receive, but also with the data they do not have, to an extent filling in some of the blanks.

[22] Riley, L. (1992). *Working paper X: Counterterrorism in Western Europe: Mechanisms for international cooperation*. Edinburgh: University of Edinburgh, UK, p. 44.

[23] As described by L. Lohnmann of the German Bundeskriminalamt (BKA) in HCHASCR 363-II, p. 43.

[24] The PWGOT has been comprised of this membership from its beginning.

[25] The European Liaison Section of the MPSB was set up in January 1976, and in 1977, it was formalised with its incorporation into Trevi. The ELS was given the responsibility of liasing with UK Constabularies and the Special Branch equivalents and security services in other EU countries after Scotland Yard's Anti-Terrorist Branch found that there was no easy mechanism for contact with other EC police forces in its investigations of international terrorist incidents: ". . . a dedicated unit, staffed by linguists . . . in order to obtain speedy responses to anti-terrorist matters" (HCHASCR 363-I, 42). Being police officer orientated, the ELS works in closer tandem with the PWGOT and was responsible for the first instance of Spanish and French police officers giving evidence in a British terrorist trial involving the PIRA, by assisting Royal Ulster Constabulary (RUC) officers in interviewing witnesses in these countries in relation to the murder of two British Army corporals in Belfast on March 13, 1988. The ELS network includes the EU 15 plus Gibraltar, Norway, Malta, and Switzerland.

[26] Bresler, F. (1992). *Interpol*. London: Penguin Books Ltd., p. 162.

[27] The significance of British opposition was because Britain has been a leading proponent of police cooperation within Europe and was the force behind the creation of Trevi.

[28] Verbruggen, F. (1995). Euro-cops? Just say maybe. European lessons from the 1993 reshuffle of U.S. drug enforcement. *European Journal of Crime, Criminal Law and Criminal Justice.* 2, *3*, pp. 150-201, p. 192.

[29] Anderson, M., Boer, M. D., & Gilmore, W. C. (1996). *Policing the European Union.* Oxford: Oxford University Press, p. 75.

[30] As do some terrorists. The Greek November 17 used the same .45 pistol when executing an assassination.

[31] Interview with Mr. Mariano Simancas, Head of Europol's Counter-Terrorism Unit, The Hague, May 2001.

[32] While the mass casualties caused by "new terrorism" attacks are indeed horrific, they are not capable of felling a stable democratic state. Even the detonation of an atomic or nuclear device is physically incapable of achieving this, as terrorists can never hope to possess the nuclear arsenal and means of delivery that a state may enjoy. A temporary state of emergency would of course exist in the event of the latter form of attack, but one would expect it to pass and democratic governance to return in due course.

Andrew Dalby is a postgraduate research assistant with the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews, Scotland. He is in his final year researching a PhD thesis on the issue of counter-terrorist structure building within the European Union. In November 2000, he presented a paper, *A Revaluation of Counter-Terrorist Strategy: Europol and the EU Role in Policing Against Terrorism*, at an International Conference on Contemporary Trends on Terrorism at the University of St. Andrews. He also presented *Running the Hydra to the Ground: The Multi Jurisdictional Approach to Policing Terrorism* for the New Jersey Association of Chiefs of Police at Wroxton College in the UK in December 2001.

Interpol: Your Best Resource for International Investigations

Mike Muth

Interpol. It's a word that many law enforcement officers have heard repeated in movies and news articles. Some think of it as a highly secret organization made up of agents who have law enforcement authority in all nations and travel worldwide in the pursuit of spies and other international fugitives on the run. The truth is that Interpol is not a secret organization and has no agents of its own, but it does pursue international fugitives as just one of the many functions it performs for 179 member countries. Interpol is in fact the radio call sign for the International Criminal Police Organization (ICPO).

The ICPO was founded in 1914 at a meeting in Monte Carlo of law enforcement officials from 24 countries. The founding principle then, as it is today, is to coordinate efforts to combat the international movement of criminals.

Interpol was never designed to be an international police force. No body of international law applies to its operation. National sovereignty is recognized, and Interpol handles "ordinary law crimes" excluding any activities that are considered military, political, racial, or religious matters; however, this does not preclude the investigation of crimes associated with a military, political, racial, or religious matter. An example would be murder committed with political motivation. From the original 24 nations that met to combat transnational crimes, the membership of Interpol today consists of 179 countries. The General Secretariat, or Headquarters, is located in Lyons, France.

Each member country establishes a National Central Bureau (NCB) to serve as the focal point for that nation's involvement in the collection of evidence, the pursuit of fugitives, locating missing persons including missing children, the identification of unidentified bodies, and the exchange of or request for information related to law enforcement investigations across international borders. In the United States, the USNCB in Washington, DC, is part of the U.S. Department of Justice and is coadministered by the Treasury Department.

The USNCB has five separate law enforcement divisions and is staffed by 95 detailed agents and permanent personnel. Most federal law enforcement agencies have one or more representatives detailed to the USNCB. There is also a detailed state police officer who represents local and state law enforcement concerns and coordinates Interpol incoming and outgoing requests with 55 liaison offices in each state, American Samoa, the District of Columbia, New York City, Puerto Rico, and the U.S. Virgin Islands. These offices are typically located within a state police or state bureau of investigation office. The traffic coming through the USNCB is

about 65% foreign requests and 35% domestic requests for overseas assistance by U.S. local, state, and federal law enforcement agencies.

So if Interpol has no agents of its own, who handles the requests? How do you seek information related to an investigation or background check from a foreign country? How do you get a lookout broadcast worldwide for a murder suspect who may have fled the country? What do you do to track the movements of a suspected criminal across international borders? How can you look for a missing child overseas? What needs to be done to make humanitarian notifications in a foreign country?

These are legitimate concerns for U.S. law enforcement personnel as well as law enforcement officers the world over. Our borders have diminished through various trade and travel agreements and have electronically been breached with the Internet. As never before, law enforcement officers need to know how to utilize the resources they presently have at their fingertips to accomplish their mission across borders. If you have the authority to run a National Crime Information Center (NCIC) check and conduct investigations, then you have the same authority to request an international check through Interpol and to request international investigative assistance.

However, requests to Interpol must come from a law enforcement agency. Interpol cannot honor private investigative requests. The requesting investigative agency either must have assigned or will assign a case number to the matter.

Furthermore, the request must make clear the type of investigation (e.g., missing person, murder) and the relevance of the information requested to that investigation.

Interpol conducts its business for law enforcement agencies through a secure telecommunications system linking the NCBs of member countries.

Many types of investigative assistance can be obtained through Interpol channels if that type of information is available to police officers in the requested country without compulsory process. Depending on the law of the country in question, this may include assistance with alien smuggling, immigration fraud and travel document forgery, drug and precursor chemical investigations, credit card fraud, recovery of stolen artifacts and art, stolen vehicle exportation/importation and traces, witness interview requests, telephone subscriber information, firearms and explosive traces, international vehicle registration/driver license checks, hotel registration and real estate ownership checks, criminal record checks, fingerprint identifications, disaster victim notifications, and other humanitarian requests.

Interpol also has unique, powerful tools for tracing fugitives internationally. They are known as Fugitive Diffusions and Red Notices.

Each Interpol NCB can issue a Fugitive Diffusion. This is nothing more than an international All Points Bulletin (APB). It can be broadcast to all other 178 countries from the requesting country or limited to one or more of nine geographic zones around the globe. A Fugitive Diffusion requests the location of a fugitive and notification back to the requesting country so that it may, if appropriate, make a

formal request for the fugitive's provisional arrest with a view toward extradition. If the Fugitive Diffusion does not result in an apprehension within several months, it should be followed up with an application for a formal Red Notice. The Red Notice is a wanted notice, with the fugitive's photograph and fingerprints, saying that the requesting country seeks the fugitive for extradition and providing full details on charges or conviction and warrant information, as well as prior arrest and conviction information.

The NCB approves and forwards your Red Notice application to the Interpol Secretariat in Lyons. This issues Red Notices in Interpol's four official languages (Arabic, English, French, and Spanish) and sends them to all Interpol NCBs worldwide. This, in turn, puts your fugitive in the border lookout systems of 179 countries.

There are a few requirements for issuance of a Fugitive Diffusion or Red Notice. There *must* be an arrest warrant. The offense must carry more than a year's imprisonment. Furthermore, the prosecutor's office must agree, in cooperation with the U.S. Department of Justice, Office of International Affairs, Fugitive Unit, to immediately draft a request for a provisional arrest with a view toward extradition for transmission when the fugitive is located. The prosecutor's office must also agree to prepare the extradition request within the time frame designated by treaty, and to pay any costs associated with extradition. Costs may include translation of the extradition request and transportation. All international extraditions are coordinated through the Justice Department's Office of International Affairs, telephone (202) 514-0000; telefax (202) 514-0080; 24-hour Department of Justice Command Center telephone (202) 514-5000.

Note: If you have obtained a Fugitive Diffusion or Red Notice and if for any reason you no longer seek or will no longer prosecute that fugitive, immediately notify the USNCB and the Office of International Affairs in writing. We need to notify the Interpol Secretariat and other Interpol members in order to prevent any foreign detention, even briefly, of a person who the prosecutor will not extradite.

Seventy-two countries treat a Red Notice as a formal request for provisional arrest with a view toward extradition if the requesting and requested countries have a bilateral extradition treaty that covers the offense(s). The United States cannot recognize a Red Notice as a request for provisional arrest but does enter other countries' Red Notice fugitives in NCIC if the U.S. has an extradition treaty with the requesting country and if the Red Notice itself contains all of the information that NCIC requires. If you find an individual who is the subject of a Red Notice, do not arrest simply on the Red Notice. Notify the USNCB immediately so that it can inform the requesting country to start the extradition process if possible. Make sure that you indicate whether the fugitive is being held on U.S. charges.

Interpol also issues a number of other unique law enforcement notices and alerts.

The Blue Notice seeks information (identity, criminal record) for subjects who have committed crimes. It is also used to trace and locate witnesses or subjects where extradition may be sought.

Green Notices provide information on career criminals who are likely to commit offenses in several countries (habitual offenders, child molesters, pornographers).

Yellow Notices seek the location of missing or lost persons, including children who are the victims of abductions. In an international abduction case, therefore, you should request both a Red Notice on the abductor and a Yellow Notice on the child.

Black Notices seek the identification of unidentified dead bodies or deceased individuals who may have used false identification.

Stolen Property Notices circulate the details and descriptions of all types of stolen property.

Purple Notices provide the details of unusual *modus operandi*, including novel concealment methods.

Gray Notices provide information on various organized crime groups and their activities.

Orange Notices provide information on criminal activity with international ramifications, but not involving a specific person or group.

Funds Derived from Criminal Activities (*FOPAC*) bulletins provide money laundering information.

So whom do I contact to assist me with my international investigation? As previously mentioned, an Interpol office has been established in each state as well as in American Samoa, the District of Columbia, New York City, Puerto Rico, and the U.S. Virgin Islands. The State of Illinois State Liaison Office contact information is (217) 557-4242, fax (217) 557-2557, ORI: IL0844300.

This office has trained investigative personnel to assist you with processing your Interpol requests. If for some reason the personnel at these offices are unavailable and an emergency exists, you may contact the USNCB directly 24-hours-a-day, 7-days-a-week at (202) 616-9000, fax (202) 616-8400, or ORI: DCINTER00.

General Information and Special Considerations for Interpol Requests

Names are almost always listed as (LAST), f/n (First name) (Middle Name). An example would be SMYTH, f/n Robert Neal. Certain cultures, including the Hispanic, may use the father's last name as the second of the three names and use the mother's last name as the third name. In such cases, indicate that the second name is the father's last name. Almost all other countries utilize a dd/mm/yyyy listing for dates of birth. Spell out the month in every date. For example, a proper date of birth to transmit overseas would be 03 MARCH 1965.

Social security numbers are seldom good identifiers outside the United States, although they may supply supplemental identification. Make every effort to obtain passport information. Information on U.S. passports is available through the U.S. Department of State, Passport Branch at (202) 647-7277.

Do not use abbreviations in your descriptions. Other countries may confuse Mt. (mountain) as the abbreviation for Montana. Spell it out.

It is the policy of the United States not to communicate with Interpol member countries that support state sponsored terrorism (i.e., Cuba, Iran, Iraq, Libya, the Sudan, and Syria, or with nonmember countries like North Korea). If you have an urgent investigative need for information from one of those countries, however, an exception will be evaluated on a case-by-case basis in conjunction with the U.S. Department of State.

If you are requesting information overseas in relation to a background/applicant check, you should include a waiver or release from the applicant. Many countries, under their privacy protection laws, require the waiver/release before they can honor the request.

Do not expect a timely response from all countries. Though the communications with these countries are state-of-the-art, and although all Interpol NCBs are to be staffed 24-hours-a-day/7-days-a-week, their internal workings, automation, and manpower deployments may preclude an immediate response. Please be patient.

Some countries will not extradite their citizens. Should you still ask the Interpol USNCB to transmit a Fugitive Diffusion on a fugitive who has fled to a nonextraditing home country or to a country with which the United States lacks an extradition treaty, and should you still apply for a Red Notice? The answer is unequivocally "yes."

Many an international fugitive has been apprehended and returned to the United States because the fugitive traveled to a country other than his or her own and was apprehended crossing the border. Furthermore, countries may decide based on criminal history in a Fugitive Diffusion or Red Notice that they can either deport or surrender a fugitive by other legal means. The bottom line is that you should utilize all means at your disposal to apprehend the fugitive, regardless of the initial degree of success.

U.S. law enforcement arrests thousands of foreign nationals annually. May foreign nationals have special rights, and does U.S. law enforcement have special obligations in such cases? The answer to both questions is "yes." The latest publication from the Department of State on Consular Notification and Access provides a complete explanation of these rights and obligations, together with the necessary notification forms in a variety of foreign languages.

Each state Interpol office has this publication, but the quickest way to get your copy is to download it directly from the Department of State website at <www.travel.state.gov/consul_notify.html>.

Caution!

- **Do not** make direct contact with potential witnesses or suspects, from the United States, through electronic or telephonic means. You may be violating the criminal laws or sovereignty of the country in which this person is located. Some

countries consider this a serious offense, and individuals in those countries may only be questioned by a representative of their government.

- The "Specialty" Rule is an international principle in all U.S. extradition treaties that says a person may only be tried and sentenced for offenses for which extradition has been granted, and extradition can only be granted for offenses that have been requested. **It is extremely important to coordinate with other local, state, or federal departments on extradition requests to ensure that all charges are part of the extradition process.** Additionally, review the final extradition order to determine if extradition has been denied for any offenses, which would preclude a trial and sentencing on those charges. Additional information on this issue is available through the Office of International Affairs at (202) 514-0000.

International Driving Permits

The USNCB has received an increasing number of requests from U.S. law enforcement agencies questioning the validity of the numerous fraudulent "International" Operating Permits being advertised across the Internet for those individuals seeking to avoid points or hide their real identity. This section seeks to explain the difference between legitimate international driving permits issued to foreign nationals operating vehicles in the United States and fraudulent international driving licenses being bought over the Internet by U.S. citizens to avoid identification and traffic adjudication, among other things.

- Legitimate International Driving Permit

  Under the United Nations Convention on Road Traffic, signed on September 19, 1949, nations agreed to recognize International Driving Permits for visiting foreign nationals **only**. This international driving permit is **not** an identity document. It is a supplement to a government issued driver's license from the driver's country of origin; however, it is the only document needed for the foreign national to operate a vehicle in the United States. Some countries do not issue a government operator permit. The United States is a signatory to this Convention and recognizes international driving permits used by foreign nationals visiting the United States. The international driving permit is a paper document, not laminated, and conforms to a design involving size, language, and color (gray only) outlined in Annex 9 and 10 of the Convention. The International Driving Permit in no way provides any immunity to foreign nationals, excepting those with Diplomatic Immunity who will have a permit issued by the U.S. Department of State, from arrest for serious violations of U.S. traffic laws. Appropriate enforcement action can be taken against foreign nationals for violations of motor vehicle laws. Officers coming into contact with foreign nationals claiming diplomatic immunity and not possessing the appropriate documents, can verify immunity status at (202) 647-7277 (24 hours).

  Any foreign national arrested or detained by U.S. law enforcement for any offense, **must** be advised of his or her Consular Notification Rights pursuant to international law as outlined above. U.S. law enforcement officers have the right to request supplemental identification from a foreign national operating

on an international driving permit. This should be a passport; however, note that passports may have been left in hotel rooms or luggage, and it is **not** a requirement that they be carried with an international driving permit.

International driving permits are only valid for citizens of another country operating a vehicle in the United States. They are not a valid permit for U.S. citizens operating vehicles in the United States. Officers presented with an international driving permit by a U.S. citizen should take the appropriate enforcement action. Many violators will attempt to fool the officer by showing a list of countries, including the United States, which have ratified the UN Convention on Road Traffic.

International driving permits are only issued by not-for-profit organizations such as the American Automobile Association (AAA) or the American Automobile Touring Alliance (AATA) for U.S. citizens intending to travel abroad. These same types of organizations overseas issue foreign nationals international driving permits for their citizens to operate in the United States. International driving permits are valid for one year from date of entry into the United States. Any traffic violations (violator "liable to proceedings") or serious traffic accidents involving foreign nationals should be reported to ORI: DCDOS015V.

- United Nations "International Driving Permits/Licenses"

  No such permit exists. The 1949 UN Convention on Road Traffic neither requires nor permits the use of the United Nations name or emblem on drivers' licenses issued pursuant to the Convention. Furthermore, the United Nations has never allowed or permitted its name or emblem to be used for such purposes. Officers presented with such a document containing the United Nations name or emblem should consider it to be fraudulent. Those in possession of such documents are seeking to avoid identification; officers need to take the appropriate enforcement action. **Note:** Legitimate international driving permits (Part Section A. of this topic) refer to the 1949 United Nations Convention on Road Traffic and contain the name of the United Nations only in this context. The use of the United Nations name in this limited context does not constitute a fraudulent use.

- Other "International" Driving Permits

  Numerous variations of "International" driver's licenses are being sold over the Internet and through other means. Some imply that they have been issued under the aforementioned Convention on Road Traffic and name a nonexistent country. Examples might be The British West Indies (nonexistent) or Macronesia (nonexistent and a variation of the geographical area of Micronesia in the Western Pacific). In addition, certain groups may issue an international driver's license for their members seeking to avoid penalty or identity.

  The only valid international driving permit has been described above. All others are false, and no international driving permit is valid for U.S. citizens operating within U.S. borders. If presented with such a document, officers should take appropriate enforcement action knowing that this may be an attempt to avoid identification and traffic penalties.

- Diplomatic Operator Permits

  The U.S. Department of State issues driving permits to all diplomatic personnel operating vehicles in the United States. This is a valid operating permit for those individuals. These personnel are required to carry a diplomatic identification card issued by the Department of State that outlines their immunity with regard to traffic infractions. All traffic violations, copies of issued traffic citations, and any accident reports, involving diplomatic personnel need to be reported to fax (202) 895-3646, ORI: DCDOS015V.

- Summary of International Driving Permits

  The proliferation of fraudulent operator permits continues to grow. All law enforcement personnel should be made aware of the contents of this section. In addition, the following is requested:

  1. Any seized fraudulent international driving permits/licenses that are no longer needed for court purposes can be forwarded to the State Liaison Division, Interpol-USNCB, Washington, DC 20530.

  2. Law enforcement officials are asked to notify local business establishments, especially those dispensing alcoholic beverages, that any international driving permit is not to be considered an identity document.

  3. A few nations have reciprocal agreements with the United States or a state that recognizes a government-issued license as a valid license to drive in the other's country (i.e., Belgium, Pennsylvania-France). For the most part, foreign nationals utilize the legitimate international driving permit outlined above.

  4. Officers coming into contact with foreign nationals who produce their government-issued license and have questions concerning the country of origin, can contact the Interpol-USNCB at (202) 616-9000 (24 hours) for country name verification or the Department of State at (202) 647-7277 (24 hours). The USNCB can only confirm the country name, not the validity of the license.

Questions concerning international driving permits may be directed to the Interpol-USNCB, State Liaison Division at (202) 616-1051 or the Department of State Fraud Liaison Section at (202) 895-3519 during normal business hours.

Conclusion

You belong to an elite global fraternity that has sworn to serve and protect. These duties may involve asking your brother and sister officers in a foreign land for assistance as well as receiving requests from officers far across oceans and time zones.

Regardless of the country of origin, put your best foot forward in honoring these requests. Each and every one of you is part of the Interpol network. Interpol is highly regarded throughout the world and will continue to serve as your best

resource for conducting international investigations. It will only enhance your ability to locate and apprehend criminals who seek refuge in foreign lands.

If you need further information, please contact your territory/city/state Interpol office, or contact my office at the USNCB, State Liaison Division, at the numbers listed above, and remember, Interpol gives **you** the ability to conduct international investigations and inquiries . . . **use it**.

Mike Muth is the assistant chief in charge of the USNCB State and Local Liaison Division and a former lieutenant with the Maryland State Police. Prior to retirement from the State Police, he served for 29 years in patrol, investigation, administrative, inspection, aviation, intelligence, and special operations assignments. He is a former commissioner with the Commission on Accreditation for Law Enforcement Agencies (CALEA) and has held numerous executive board positions with both state and national law enforcement associations. The Interpol-USNCB State and Local Liaison Division is responsible for coordinating operations between 18,800 U.S. State and Local law enforcement agencies and their foreign counterparts in the other 178 Interpol member countries through 55 separate State Liaison offices in each state, territory, New York City, and Washington, DC.

Understanding Islam in Light of the Attacks on the World Trade Center and the Pentagon

Labib Mickhail, PhD

The barbaric, horrific terrorist attacks on Tuesday, September 11, 2001 on the World Trade Center in New York and the Pentagon in Washington, DC have caused every American to ask, "Why did it happen? Who did it? And why do they hate us?"

The investigation of the CIA and FBI has concluded that the attackers were Muslims. Does that mean that every Muslim is a terrorist? By no means. There are many decent Muslims, but while many news commentators and politicians are proclaiming that Islam is a peace-loving religion, others are warning of Islamic Jihad, or Holy War.

These conflicting descriptions of Islam can be explained by examining the three types of Muslims: (1) secularists, (2) moderates, and (3) fundamentalists. The Koran, the holy book of Islam, is used by each group to justify their way of thinking.

Three Types of Muslims

Secularists are Muslims who do not have a knowledge of the contents of the Koran and only know a verse or two to justify enjoying their life such as, "Wealth and children are the adornment of the life of this world" (Surat AI-Kahf 18:46).

Moderates know the Koran but seek to make their faith relevant to modern life. They try to reconcile the contradicting verses in the Koran in such a way that Muslims may tolerate Jews and Christians living among them. They emphasize the verses that came to the Prophet Muhammad when he was weak militarily and in need of the support of Jews and Christians. These verses which are kind to Jews and Christians are as follows:

> So, if you (Muhammad) are in doubt concerning that which We have revealed unto you then ask these who are reading the Book [the Torah and the Injeel (Gospel)] before you. Verily the truth has come to you from thy Lord. So be not of those who doubt? (Surat Yunus 10:94)
>
> Verily, you will find the strongest among men in enmity to the believers (Muslims) the Jews and those who are AI-Mushrikun, and you will find the nearest in love to the believers (Muslims) those who say: "We are Christians." That is because amongst them are priests and monks, and they are not proud. (Surat Al-Maidab 5:82)
>
> Verily, those who believe and those who are Jews and Christians, and Sabians, whoever believes in Allah and the Last Day and does righteous good deeds

shall have their reward with their Lord, on them shall be no fear, nor shall they grieve. (Surat Al-Baqarah 2:62)

Barnabas Fund in England wrote . . .

> The Muslim Prophet Muhammad, the founder of Islam, was a complex character whose attitudes and opinions changed and evolved during his lifetime in response to events around him. It is not surprising to find that Islam is a complex faith.

When needed, Muslim clerics use Koranic verses including those kind to Jews and Christians to paint a glowing picture of Islam as a religion of peace, brotherhood, modesty, morality, self-discipline, and family values, but, the true face of Islam is revealed in the Koranic verses calling Muslims to "Jihad," which means holy war against all non-Muslims. Barnabas Fund later stated in his article . . .

> "It is true that many individual Muslims are peace loving and law-abiding. But, it is not true that peace is the main characteristic of the faith of Islam."

Fundamentalists are those who want to apply the more extreme verses of the Koran to the letter. These verses came to Muhammad after he was strong militarily and after he realized that the Christians and Jews were not becoming followers of his new religion. Muhammad's anger in the following Koranic verses, which abrogate the nice verses in the Koran, is the root of violence which saturates and captures the minds of these fundamentalist Muslims:

- **The Prophet Muhammad urges Muslims to fight in the cause of Allah.**

  The prophet Muhammad urge the believers (Muslims) to fight. (Surat Al-Anfal 8:65)

  Jihad (holy fighting in Allah's cause) is ordained for. (Surat Al-Baqarah 2:216)

- **The Koran commands Muslims not to befriend Jews or Christians.**

  O ye who believe (Muslims) take not the Jews or the Christians for your friends and protectors. They are but friends and protectors to each other. And he among you that turns to them (for friendship) is of them. (Surat AI-Maidah 5:51)

- **The Koran commands Muslims to fight Jews and Christians.**

  Fight against those who believe not in Allah, nor in the Last Day, nor forbid that which has been forbidden by Allah and His Messenger (Muhammad) and those who acknowledge not the religion of truth (Islam) among the people of the Scripture (Jews and Christians) until they pay the Jizyah with willing submission, and feel themselves subdued. (Surah At-Taubah 9:29)

Jizyah is a special high tax to be paid only by Jews or Christians who do not want to renounce their religion and convert to Islam.

- **The Koran commands Muslims to fight non-Muslims until they exterminate all other religions and Islam would be the only religion in the world.**

  And fight them until there is no more Fitnah (disbelief and worshipping of others along with Allah) and (all and every kind of) worship is for Allah (alone). But if they cease, let there be no transgression except against As-Zatimun (the polytheists and wrong doers). (Surat AI-Baqara 2:193)

This verse is mentioned also in Surat AI-Anfal 8:39. Because of the misunderstanding and ignorance of Christianity, Muslims believe that Christians are polytheists, because they believe in a Triune God. Fundamentalists look at Jews and Christians and all non-Muslims as infidels who must be killed because they have no value as human beings and must be exterminated from the face of the earth.

Fundamentalists divide the world into two camps: (1) Dar Al-Harb' (Camp of war) where Jews and Christians live and (2) Dar AI-Sallam (Camp of peace) where Muslims live. They believe that holy war against those who live in the camp of war should continue until they are exterminated.

Fundamentalists dream of a global Islamic empire. They believe that if they destroy America and the western countries, they will achieve this dream.

- **The Koran declares that Muslims who fight and die in battle are promised forgiveness and a sexually luxurious life in Paradise.**

  And if you are killed or die in the Way of Allah, forgiveness and mercy from Allah are far better than all that they amass (of worldly wealth). (Surat AI-Imran 3:157)

  Verily, Allah has purchased of the believers their lives and their properties for (the price) that theirs shall be the Paradise. They fight in Allah's Cause, so they kill (others) and are killed. It is a promise in truth which is binding on Him. (Surat At-Taubah 9:111)

What can martyrs expect in paradise? The Koran describes life in paradise in the following words:

  Eat and drink with happiness because of what you used to do. They will recline (with ease) on thrones arranged in ranks. And We shall marry them to Hur (fair females) with wide lovely eyes. And We shall provide Them with fruit and meat such as they desire. (Surat At-Tur 52:17-20,22)

  Water flowing constantly and fruit in plenty whose supply is not cut off and reclining on couches raised high, verily we have created them (women) of special creation and made them virgins of equal age. (Surat AI-Waqiah 56:31-37)

  Gardens and vineyards and young full-breasted virgins of equal age and a full cup of wine. (Surat An-Naba 78:32-34)

Some prominent Muslim clerics call the suicide bombers martyrs because in the Koran, a martyr is guaranteed total forgiveness of his sins and eternal life in paradise where he can drink wine and will be married to a great number of beautiful sensual virgins. While in fact these martyrs are nothing more than murderers.

Nineteen educated Muslims committed suicide and killed thousands of innocent men, women, and children in the World Trade Center, the Pentagon, and the four planes they flew on that black Tuesday. Those nineteen Muslims did that because of their deep conviction that they will go directly to paradise to enjoy sensual pleasures and because of their terrible hatred for America, a country populated by a Christian majority.

Muhammad Atta, who flew the first plane into the World Trade Center, was a devout Muslim. He was born in Egypt to a lawyer and was a highly intelligent person who communicated with ease with children, old men, professors, and people in government. As a student in Germany, he was known to be quiet and very religious. Atta regularly prayed on the floor of his office and founded an Islamic prayer and study group at the University in January 1999.

Atta lived and moved easily in Western society while secretly hating it. He was a man on a mission and on the front of his thesis, presented in October 1999, he wrote the following verse from the Koran: " My Prayer and my sacrifice and my life and my death belong to Allah, the Lord of the worlds" (Washington Post 09/22/01). The West needs to know that many other Muhammad Attas may be quietly living amongst us.

- **The Koran commands Muslims to terrorize and torture and kill anyone who disobeys Allah and the Prophet Muhammad.**

  (Remember) when your Lord revealed to the angels, "Verily I am with you, so keep firm those who have believed. I will cast terror into the hearts of those who have disbelieve, so strike them over the necks and smite over all their fingers and toes. This is because they defied and disobeyed Allah and His Messenger (Muhammad). And whoever defies and disobeys Allah and His Messenger, them verily, Allah is Severe in punishment. This is (the torment), so taste it; and surely, for the disbelievers is the torment of the Fire." (Surat AI-Anfal 8:12-14)

  The recompense of those who wage war against Allah and His Messenger (Muhammad) and do mischief in the land is only that they shall be killed or crucified or their hands and feet be cut off from opposite sides, or be exiled from the land. That is their disgrace in this world, and a great torment is theirs in the Hereafter. (Surat AI-Maidah 5:33)

- **The Koran declares that Allah loves those who fight in His cause.**

  Verily, Allah loves those who fight in His Cause in rows as if they were solid structures. (Surat As-Saff 61:4)

- **The Koran commands Muslims to convert non-Muslims to Islam by force.**

> Kill the Mushrikun (polytheists, Christians, and non-Muslims), wherever you find them, and capture them and besiege them, and lie in wait for them in each and every ambush. But if they repent and perform As-salat (public prayer with Muslims) and give Zakat (Islamic alms), then leave their way free. Allah is oft-forgiving, most merciful. (Surat At-Taubah 9:5)

Mathematician Blase Pascal who lived in 1670 said, "Men never do evil so completely and cheerfully as when they do it from religious conviction." The heart of man is naturally evil. You can ignite that evil with religious gasoline. The Koran's verses ignited that evil in the hearts of those terrorists and will ignite evil in many more Muslims' hearts.

While violence committed by militant Muslims is sanctioned and commanded by the Koran, any atrocities committed by Christians were never sanctioned by the New Testament commandments. Jesus Christ commanded His apostle Peter,

> Put your sword in its place. For all who take the sword will perish by the swords. (Matthew 26:52)

Freedom of Thought in Islam

Islam is a prison with no way out. Once a person enters that prison, it is impossible to leave it alive.

> Then what is the matter with you that you are divided into two parties about the apostates? Allah has cast them back (to disbelief) because of what they have earned. Do you want to guide him whom Allah has made to go astray? And he whom Allah has made to go astray, you will never find for him any way (of guidance). They wish that you reject Faith, as they have rejected (Faith), and thus that you all become equal (like one another). So take not Aouliya (protectors or friends) from them, till They emigrate in the Way of Allah (to Muhammad) But if they turn back (from Islam), take (hold of) them and kill them wherever you find them, and take neither Aouliya (protectors or friends) nor helpers from them. (Surat An-Nisa 4:88,89)

This verse means that if a person says the Islamic Shahada (creed): "I testify that there is no God but Allah. I testify that Muhammad is the Messenger of Allah," he cannot change his mind. If he does change his mind, he will be executed or beheaded as has happened many times in Saudi Arabia, Afghanistan, and other Islamic countries.

Islam is a religion of intellectual censorship.

In Islam, the democratic right to free thought and individual decision concerning religious matters is totally denied. We have more than one example of that intellectual censorship.

The first is Salman Rushdie. Salman Rushdie was born to a Muslim family in Bombay but has spent much of his life in London, England. He wrote a book

entitled *The Satanic Verses*. Muslims thought this book was an insult to the Prophet Muhammad and Islam, so Ayatollah Ruholla Khomeini issued an order to assassinate Rushdie and promised $5 million to the one whom would kill him. Khomeini, Iran's spiritual leader at that time, said in a statement read for him on the radio in 1989: "Anyone who died attempting to kill Rushdie," he promised. "would go straight to paradise."

The second is Dr. Farag Foda, the great author who was assassinated in Cairo, Egypt in 1993 because he wrote many books exposing the true face of Islam and Islamic society. He was accused of being an apostate Muslim and was shot and killed in front of his son.

The third is Professor Nasr Hamid Abu Zeid, who was accused of being an apostate Muslim because of his books about the Koran. The court in Egypt ruled that he must divorce his wife, Ibtihal Younes. He fled from Egypt and is now living with his wife in Holland.

The fourth is the well-known Egyptian writer Naguib Mahfouz, who became the first Egyptian to win the Nobel Prize for Literature. Muslims stabbed him in front of his house in an attempt to kill him. The man is over 80 years old. They wanted to kill him because they thought that he insulted Muhammad in his novel, *The Children of Gabalawi*.

It is of great importance for any American or any secular Muslim to know what kind of society he or she will live in if fundamentalist Muslims rule. The Taliban, which used to be Afghanistan's ruling Islamic movement, is an example of this extremist militant faith, which is based on a literal interpretation of the Koran, and it shows in their way of life.

In Afghanistan, any woman who will show more than her eyes will be flogged. In Saudi Arabia, a woman is banned from driving a car or from walking down the street without covering all of her body except for her eyes.

Christians who went to Afghanistan to help the poor and the sick with food and medicine were arrested and jailed because they had bibles and Christian cassette tapes. In Saudi Arabia, Christians are banned from holding worship services let alone building a church. In the meantime, Muslims are taking advantage of the American freedom and building hundreds of mosques on American soil.

In Sudan, more than one million Christians were killed by the Islamic government in Khartoum. In Algeria, thousands of Christians were slaughtered by militant Muslims with no regard for life.

Today we are hearing on radio and television many Muslim clerics saying that Islam means peace, but the word *Islam* means "submission," and a Muslim is one who is in submission to Allah. Their goal as stated in the Koran is to bring the entire world into submission to Allah and the Koran and have a global Islamic empire.

Labib Mickhail, PhD, has written more than 60 books and hundreds of articles on Islam and Christianity in both Arabic and English. He has produced or been a guest of many radio and television programs. He holds a doctorate in theology and has pastored Evangelical churches in the Middle East and America.

Combating Terrorism: Russian Perspective

Yurii M. Antonyan, PhD
Vladimir A. Sergevnin, PhD
Diana A. Zadorskaya, PhD

"Send not to know for whom the bell tolls: It tolls for thee."

Meditation XVII, John Donne, 1624

Historical Background

Russia has a long history of coexisting with political terrorism and lives under fear of terror. Sergey Nechaev (1847-1882), for example, might be called the extremist forerunner of modern Russian terrorism. He was the father of political terror, which he developed as a revolutionary tool as early as 1869. For Nechaev, when it came to revolution, the end always justified the means. He believed that a terrorist must be

> . . . hard towards himself, he must be hard towards others also. All the tender and effeminate emotions of kinship, friendship, love, gratitude, and even honor must be stifled in him by a cold and single-minded passion for the revolutionary cause. There exists for him only one delight, one consolation, one reward and one gratification—the success of the revolution. Night and day he must have but one thought, one aim—merciless destruction. In cold-blooded and tireless pursuit of this aim, he must be prepared both to die himself and to destroy with his own hands everything that stands in the way of its achievement.[1]

This trend became even stronger ten years later when the rebel group named itself the People's Will (*Narodnaya Volya*), the name under which the radicals were responsible for the assassination of Alexander II in 1881. The objective of the group was to cause a coup or overthrow the Russian government. They believed that the assassinations would be the trigger for revolution and would finally change the order of the regime.

The Bolsheviks and Lenin inherited terrorist approaches and converted them into the state policy. The communist state developed two main types of terrorism. First, there was the internal policy of using terror for the benefit of establishing a so-called "dictatorship of proletariat." The goal was to suppress and physically eliminate opposing forces in the country and convince the population to be loyal to the new regime. In September 1918, the Russian communist government officially announced the policy of "Red Terror." Hundreds of thousands died; millions were scared.

Secondly, there was an international terrorism with the goal to cause destruction and chaos, resulting in a world communist revolution. There were many cases of state-supported terrorist actions. Soviet secret police (NKVD-OGPU-KGB) even established a special department, which was in charge of elimination of popular political figures worldwide (e.g., assassination of Leon Trotsky in August 1940).

Stalin developed terrorism as one of the most powerful tools of state policy, but individual and group terrorism were almost unknown under Stalin, Khrushchev, and Brezhnev. Isolated acts of terrorism (i.e., the explosion in Moscow's subway in January 1977) got the state security agencies' (KGB and MVD) attention, and terrorists were arrested and executed almost immediately. Everything changed under Gorbachev and Yeltsin. The collapse of the former USSR triggered criminal terrorist acts in Russia. In 1994-1995, there were 64 terrorism-related explosions. In 1996, the number increased to 886, in 1997 to 642, and in 1998 to 668.[2]

In response to increased activity of terrorists in January 1997, the Russian Government established the Interdepartmental Anti-Terrorist Commission of the Russian Federation with responsibilities to coordinate the organs of executive power: the Federal Security Service (FSB), the Ministry of Internal Affairs (MVD), the Ministry of Defense (MOD), the Federal Agency for Government Communications & Information (FAPSI), the Federal Border Service (FBS), the General Prosecutor's office, and the Premier. The prime minister and the FSB were in charge of the commission. Its goal was to coordinate the activity of the executive branch of federal government in the battle on terrorism and to increase the effectiveness of conducting special operations on prevention and suppression of terrorist activity. In order to achieve these goals, the following objectives were addressed: elaborating and conducting actions aimed to identify, prevent, and suppress terrorist activity; submitting suggestions to the Government of the Russian Federation to create a program of measures for providing safety and security for the people; and coordinating collaboration between different levels of government to establish measures to stifle terrorism.

From the very beginning, however, this commission did not have the potential to function effectively, mainly because the director of the FSB did not have enough power to meet the above-mentioned objectives. He also did not have manpower, transport, or financial and equipment resources at his disposal. In this situation, it was possible only to counteract terrorism as an illegal activity and not as a sociopolitical phenomenon.

It was important to determine and put into legislation the status of the commission, because this issue played an important role in creating a statewide system designed to counteract terrorism. It is necessary to mention that some of the powers of the commissions were to help discover and eliminate factors that create fertile conditions for terrorism to spread.

By the end of 2000, the prime minister of the government was appointed as a chairperson of the commission, and the federal security service director and ministry of internal affairs minister were appointed as his deputies.

Only after such appointments was it possible to make the decisions necessary in order to organize and improve cooperation of federal executive institutions in preventing, suppressing, and liquidating consequences of terrorist acts; request necessary information from state authorities and from federal executive authorities; and encourage involvement (with the permission of their supervisors) of specialists from different plants, establishments, institutions, and organizations to assist in preventing, suppressing, and eliminating results of terrorist acts.

Anti-terrorism actions in Russia were organized on three levels:

1. Prime minister – responsible for the general policy on counter terrorism

2. Security ministries [FSB, MVD, SVR, Federal Protective Service (FSO), MOD, and the FBS] and ministries responsible for preventive measures (the Ministry of Nuclear Energy, the Ministry of Transport, and the Ministry of Emergency Situations)

3. Field offices of FSB in the cities and states and regional administrations of Combating Organized Crime of the MVD

The Interdepartmental Anti-Terrorist Commission coordinated all counter-terrorist actions and is responsible for setting up the operational personnel in each individual case. No one was permitted to overrule its decision during the operation.

The FSB had at its disposal Directorate A (the former "Alfa" unit), responsible for taking measures against terrorists on means of transport and buildings. Directorate B (the former "Vympel" unit) was to react in strategic installations, which is what they were originally trained to do for their missions abroad. Both Directorates were expected to act together in large-scale operations. Special operations departments were set up by the FSB in 11 cities.

In 1999, Islamic justice was established in Chechnya. Terrorism, including a series of bombings in Moscow (several hundred people were killed there), erupted. After that, several thousand Islamic militants, armed members of a Chechen Muslim fundamentalist group whose aim was to merge Dagestan with neighboring Chechnya in a single Islamic state, invaded Dagestan. Russia responded with police and military attacks by federal forces, and the militants retreated; the incident contributed to Russia's decision to invade Chechnya later in 1999. International extremist organizations, including Osama bin Laden and other criminal associations, back the Chechen terrorists. The territory of Chechnya is used to host and train terrorists from Arab countries and some Western European countries. The numerous terrorist groups are free and go unpunished and make raids in the territory of Russia. In 1999, there were 20 terrorist acts in the Russian Federation registered by MVD. In 2001, representatives of terrorist organizations were registered by FSB in 49 of 89 states in Russia, and in 2001, the terrorist groups twice attempted to gain access to Russian nuclear munitions dumps. Security agencies do not exclude the possibility that terrorist groups may directly attack nuclear installations.

In June 2000, the Anti-Terrorist Center of the Commonwealth of Independent States (Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan) was established with the purpose of coordination of counter-terrorism measures on the territory of the former Soviet Union. In November 2001, the main organized crime administration of the criminal police service at the MVD established a special section on fighting terrorism and extremism. National police offices in the seven federal districts have already set up terrorism sections. The officers intend to cooperate with foreign law enforcement bodies in carrying out anti-terrorist activities.

Defining Terrorism

Arguments regarding terrorism and its notions, forms, and methods have been going on for a long period of time. There is no doubt that it is a dangerous socio-political phenomenon. Because terrorism is built on violent criminality, its levels and forms are represented as a rate of public morality from one side, and from another side as a rate of societal and national effectiveness of efforts, aimed to resolve critical problems, which lead to the creation of terrorism—that is terrorism prevention.

In spite of the scale and severe consequences of terrorism, society and especially local governments in the provinces and law enforcement were ill-prepared to deal with it. The Russian security system's unpreparedness to tackle terrorism and its late reaction took place because of shortcomings in the functional goals of its anti-terrorism institutions and because of the attempts to use the same pattern of counteractions with acts of terrorism which were different in scale, content, goals, and motives than those of the past.

It is impossible to create a protection mechanism for terrorism without analyzing its nature and genesis. This phenomenon still needs further research in spite of the fact that Russian mass media, different publications, and scientific literature have paid a lot of attention to terrorism.

The nature of terrorism in Russia is old. Terrorism was always the weapon of political, religious, and criminal outcasts who had a lack of resources and humanitarian values and an extraordinary desire to exercise power over people and society. Because of this powerlessness, they turned their hopes towards a great liberator who some day will come and accomplish his mission by an endless line of violent acts. Wide spread organized crime and the instability of economic and social conditions—high unemployment and job insecurity, friction among ethnic groups and between urban populations and job-seeking migrants to cities, and a general decline in the standard of living—are contributing to terrorism in Russia. Production disorganization, social system destruction, nonpayments of paychecks—these and other factors create conditions for social self-defense and lead to the development of anti-state terror.

Neither the *Criminal Code of the Russian Federation* nor the *Law "On terrorism"* reflected the current reality of the terrorist threats. There is no single, universally accepted, definition of terrorism.

Russian legal definition is based on the *Criminal Code*. Terrorism is defined in the *Criminal Code* (Article 205) as "the acts of creating danger of human vanishing, seriously damaging the property . . ."[3] The definition causes serious doubts. The most confusing is the definition written in the Law "On terrorism," which is much broader than the one in the *Criminal Code*. Some terrorist features are not yet determined. Legal typology doesn't correspond with reality, which prevents adequate understanding of the nature and reasons for the phenomenon.

The analytical definition approaches terrorism as a social and political phenomenon. From this perspective, terrorism is the socially and politically motivated, ideologically approved usage of violence or the threat of usage of violence with the purpose to manipulate human behavior and illegally reach goals.

Goals are diverse but can be grouped into the following categories:

- Political – change of regime, overthrow the government, *coup de tat*, damage relations between the countries, disgrace to political system, and so on
- Social – upset social order
- Economical – damage to economical order; upset the budget; interrupt vital supplies, like oil, gas, electricity
- Ethnic and religious – fundamentalist sects, racism, genocide, spread of new beliefs
- Ideological – communism, nazism, spread of ideas
- Psychological – spread fear, demoralization, hatred, suspicion
- Ecological

There are three basic forms of terrorism:

1. Individual terrorism often has criminal motivation (e.g., revenge, intimidation, and any other personal motives). It is difficult to detect this form of terrorist.
2. Group terrorism requires organization and some type of leadership, recruitment, and retention of members.
3. State terrorism is one of the political tools utilized by a government, which establishes a specific agency or uses a legitimate state institution for gaining domestic or international benefits for the regime.

Some characteristics of terrorism, which are mentioned in the Law "On terrorism" need to be accepted by the *Criminal Code*. First of all, it needs to address the propaganda of terrorism. Its danger is connected with attempts to gain public approval of a terrorist activity as a form of political fight, with substantiation of its legal use and also with direct initiative calls to terrorist activities, which may lead to real commitment of criminal actions and involve separate individuals or groups committing severe violent crimes. These appeals are realized verbally or by distributing written or visually demonstrative materials.

Secondly, it is a creation of terrorists' organizations. This form of terrorist activity began to spread in the second half of the 20th century with the increase in the number of terrorist organizations and the expansion of social support for terrorism. This form of terrorist activity involves hiring participants to different terrorist organizations, personnel training on methods and ways of conducting terrorist acts, and preparation for the forthcoming terrorist acts—rehearsals of terrorist acts, separate stages of terrorist operations, and so on. This form also involves establishing contacts with other terrorist organizations and creating and maintaining connections with organized crime institutions, representatives of illegal firearms businesses, and drug dealers. A high level of secrecy and specialization of terrorist group participants according to different functions (e.g., hiring personnel, recognizers, warriors,

production specialists of combat substances and cover documents, secret apartment maintenance staff) is common for organized terrorist activity.

Thirdly, it is assisting terrorist organizations. With the creation of large terrorist institutions, this form is becoming more important in the overall system of terrorism. Main variations of this form of terrorism are extremist groups financing and providing the means for terrorism, providing facilities for training their members, and harboring and hiding them after committing terrorist acts. This form of terrorism can be used by states (so called terrorism sponsors) as well as by representatives of business circles and ethnic and other social groups that express sympathy to terrorist organizations or support them because of their common political interests or direct involvement with extremist organizations in conducting tasks of legal political institutions to influence their enemies.

Terrorism Prevention

Modern history of terrorism shows that it is not realistic to eliminate it or to control it, but it is possible to reduce it. For this purpose, it is not enough to just improve anti-terrorism legislation to solve the problems created by terrorism in Russia. This is because the laws on terrorism are aimed to suppress terrorist activity and to punish those who are responsible, but it is much more important to prevent such activity from occurring in the first place. Even a successfully conducted anti-terrorist operation with the terrorists' capture and apprehension cannot compensate its damages and cannot be evaluated completely positive, because it shows missed opportunities to prevent such an act.

A lot of negative consequences occur during the preparation stage of a terrorist act. Usually other crimes are committed before a terrorist attack (e.g., burglary; illegal weapon possession; acquisition of explosives, toxins, and radioactive substances). A substantial number of groups and even layers of society are getting involved in different negative criminal consequences; social tension is increasing; international, interethnic, and religious controversies are growing; legal nihilism is spreading; and opponent aggression is increasing. Problems of crime and terrorism prevention remain unsolved in several law enforcement institutions. Director of the Federal Security Service Kovalev N.D. calls law enforcement personnel to pay specific attention to the necessity of expanding the prevention function: "The main task is to stop terrorist activity in [sic] early stages – in the [sic] preparation stage and in the [sic] stage of eliminating reasons and conditions, which create fertile soil for committing terrorists acts. We used to have such instrument[s] as early prevention. Now we don't have it any more. But we definitely need it."[4]

The most effective prevention and of course the most expensive and difficult is early prevention. Today, the Russian government focuses on several main activities which can promote terrorism prevention strategies and tactics:

1. Analyze, localize, and minimize those social, political, financial, and other factors, which create fertile ground for terrorism. It is necessary for these purposes to study thoroughly this phenomenon and its roots and reasons. Studying and explaining motives of the widespread cases of terrorism and subsequent data gathering and assessment can play an important role in determining sets of problems, that need to be solved in the near

future—economic, social, and political. Modern Russian terrorism has several different motives: political agenda (e.g., communism), religion (e.g., Islamic fundamentalism), ethnicity (Chechen), revenge, the furthering of organized criminal activity (e.g., restructuring criminal spheres by Russian organized criminal groups), and so on.

2. One of the effective remedies in terrorism prevention activities by security agencies is an implementation of programs that reward individuals for information that leads to terrorist act prevention or that leads to apprehension of people committing such acts. Several states of Russia set up conditions on which the state can buy illegal weapons from citizens without persecuting them. At the same time, rewards for information on criminal or terrorist activities are available only after terrorist acts have been committed. This doesn't help much to save people's lives.

3. Launch an information campaign designed to disclose the criminal and violent nature of terrorist groups and organizations. Build public awareness about the legal consequences of participation in any activities related to terrorism.

4. Develop public safety programs to protect vulnerable objects and locations.

5. Enhance community participation in "terrorist watch" programs.

6. Improve intelligence by increasing the cooperation between FSB and MVD forces.

7. Enhance information sharing by centralizing and increasing the protection of the integrated information system of all security forces of the Russian Federation.

8. Improve training for security forces by developing realistic anti-terrorist action scenarios and organizing regular exercises for security forces and citizenry.

9. Foster coordination between security forces and communities on the basis of model local, state, and federal plans of responding to terrorist attacks.

10. Develop a general policy of covering terrorism through the mass media. Legal issues of mass media participation in anti-terrorism activities have not been thoroughly illustrated. In the Law "On terrorism," there are only general restrictions for mass media that should be followed during the counter-terrorism operations. Law enforcement agencies tried not to broaden the scale of psychological war. If pro-terrorism statements appear, and unfortunately they do, they strengthen terrorists' courage. Agencies shouldn't mix terrorism with politics and ideology and should not depict it as an international plot against Russia as a whole. Wrongful and contradictory understandings of causes and roots of terrorism became a result of insufficient anti-terrorism actions in Russia. Most of the people connect them with Chechnya. Organizers and committers of terrorist acts in Moscow and Northern Caucasus, who were under the criminal investigation, had no direct links to Chechnya. Most of them were of Karachaevo-Cherkessia (one of the Russian provinces in the Northern Caucasus) origins.

11. Improve interethnic relations in the Russian Federation, which is a multinational and multicultural country. Even if something is being done on the federal level, it doesn't go as far as to reach provinces.

Political leaders of Russia consider counter-terrorism as one of the most important state tasks. Some of the main trends in this activity are legislative improvement, strengthening cooperation between communities and federal agencies, creation of special task forces, increasing the number of federal agencies personnel, dealing with terrorism problems, and providing better technical equipment.

Russian security agencies trying to put pressure on the forces supporting terrorism will use all available resources to the full extent including military ones to punish terrorism, to assist and collaborate with other countries, and to not allow any weaknesses in dealing with terrorists.

Endnotes

[1] Nechaev, S. (1997). Catechism of a revolutionist. In *Revolutionary radicalism in Russia*. Moscow, p. 147.

[2] Petrishev, V. E. (2001). *Zametki o terrorizme* (*Notes on terrorism*). Moscow: Editorial URSS, p. 251.

[3] *Ugolovni Codeks Rossiskoi Federatzii* (*Criminal Code of the Russian Federation*). (1996). Moscow: Novaya Volna. p. 132.

[4] Interdepartmental Antiterrorist Commission of Russian Federation. Transcript of the August 7, 1997, meeting, Moscow, p. 5.

Yurii M. Antonyan is a deputy chief for the Stavropol Institute of the Ministry of Internal Affairs (Russia). He has 25 years of experience serving the Ministry of Internal Affairs (National Police). He earned his PhD at the Ministry of Internal Affairs Academy. He has published more than 30 books and articles on organized crime and terrorism issues.

Vladimir A. Sergevnin is a research associate for the Illinois Law Enforcement Executive Institute and professor at St. Petersburg University of the Ministry of Internal Affairs, Russia. He earned his PhD at the Moscow Institute of Popular Economy in 1986. He has 24 years of teaching experience at Illinois State University, Western Illinois University, St. Petersburg University, and Vladimir Juridical Institute (Russia). He has published over 40 articles and written six books.

Diana A. Zadorskaya is a senior administrator of the international department. She earned her master of education in human resource development at the University of Illinois and her PhD in philosophy in legal sciences at Saint-Petersburg University of the Ministry of Internal Affairs (MVD). Dr. Zadorskaya is the author of eight articles.

Local and State Anti-Terrorism Analysis

Marilyn B. Peterson, CCA*

The events of September 11 and their surrounding activities, have shown us that terrorism can have a serious impact not only on the international scene, but also on local and state police operations. These events have left many local and state law enforcement executives with a question: What approach should be taken to achieve an effective proactive and responsive anti-terrorism program?

The key to an effective anti-terrorism effort is intelligence, that is, analyzed information.[1] Traditionally, police have focused on collecting and storing information, sometimes ignoring the need to analyze and draw meaning from that data. Few smaller police agencies have established intelligence units or analysts, and while the federal government is generally responsible for marshalling the response to terroristic activities, they cannot be pro-actively aware of every group in every corner of every state.

The fight against terrorism calls for locating and measuring terrorist risks, analyzing information and using intelligence to guide operations. The type of work required to respond to terrorism is virtually impossible without trained intelligence professionals. The activities suggested below assume that someone with intelligence training is available to complete these tasks.

This article provides direction on how to accomplish analysis and risk assessment regarding international or domestic terrorist activity. Anti-terrorism analysis can be broken into three steps: (1) inventory, (2) risk assessment, and (3) dissemination. These steps need to be done in the context of the agency's jurisdiction and span of responsibility. That is, not all potential groups, targets, or weapons are likely to occur within one jurisdiction.

Inventory Phase

The inventory phase combines collecting raw data with organizing and evaluating that data. The first of several sub-steps is that **potential sources of threats** must be determined. These sources may include domestic terrorist groups, such as the Aryan Nations, the Animal Liberation Front, the World Church of the Creator, or international terrorist groups including al Qaeda, the Hizballah, the Red Army Faction, the National Liberation Army, the 17 November, etc.[2] The possibility of one or two actors, such as a Unabomber or a Terry Lynn Nichols and Timothy McVeigh (Oklahoma City) must also not be overlooked.

How does one go about determining the presence of members of these groups in a particular jurisdiction? First, know the community: its make-up, its ties to other countries or particular belief structures, its potential for having extremist or terrorist group members present. Second, do basic research through the Internet or a

* The opinions expressed in this article are those of the author and do not necessarily reflect the opinions of the New Jersey Division of Criminal Justice or any other organization.

local library on these groups to determine their beliefs, locations, etc. Third, contact appropriate state or federal agencies with active anti-terrorist units which might be able to provide information on known group members in the area.[3]

For each group considered a possible threat in the area, a group profile should be completed. A group profile usually includes numerous bits of information on the organization including the following:

History
Ideology
Recruitment methods
Geographic base
Sources of funds
Significant dates
Modus operandi
Leadership
Previous tactics
Communication networks
Sympathizers
Transport methods
Current status
Structure
Goals/intent
Training/skill level
Violence potential
Weaponry available
Membership size
Travel history
Intelligence capability
Trends
Access to false documents
Sponsorship by state (country)
Connections to other groups
Other criminal acts

In addition, a review of world news should be done to determine if any recent events have occurred that might impact these groups. The events could range from attacks against their countrymen, to legal actions being taken against group members (such as trial or sentencing), to legislation being passed of which they disapprove. Another potential pre-incident activity could be the collection of funds, medicine, and clothing through nonprofit charities that end up in the hands of terrorists.

Once potential sources of threats are known or suspected, then **the potential targets** may be determined. The Animal Liberation Front, for example, may target facilities that use animals to test pharmaceutical products. Other domestic terrorists might target government facilities. International terrorists, on the other hand, are broader in their targeting and may look for symbolic targets which represent a government, the business world, or Western culture. An inventory should include what critical assets, locations, or operations within the jurisdiction might be targets for the groups that may be operating within, or travel to, that jurisdiction. Some targets that might be considered include the following:

Government buildings
Electric plants
Water supply
Defense contractors
Internet
Airports
Post offices
Mass transit
Tourist attractions
Nuclear plants
Food supply
Telecommunications
Chemical plants
Sports stadiums
Seaports
Malls

Targets of opportunity also should not be ignored. These are targets presented by special occasions (the Olympics, major celebrations), visits from dignitaries, campaign stops, etc.

For each of the sites in the jurisdiction that are considered possible targets, an honest assessment of those targets' vulnerabilities should be made. Their security levels should be noted, along with any upcoming special events, changes in security, environmental vulnerabilities, etc.

The table that follows shows a local target inventory sample. Four locations' vulnerability to attack, their current level of security, and the impact any attack might have are examined. The scores are then computed to determine which local targets are the most vulnerable and have the highest damage potential to the community.

Local Target Inventory Sample

Location	Probability of Attack	Threat to Security	Impact of Attack	Total Scoring
Reservoir	High	High	High	**High**
Tri-State Mall	Medium	Medium	Medium	**Medium**
Nuclear Plant	Medium	Medium	High	**Medium**
County Airport	Low	Low	Medium	**Low**

Probability of attack refers to the likelihood of that location being chosen as a target.

Threat to security refers to the probability that security at the location could be breached.

Impact of attack refers to the number of people who may be harmed by an attack.

Using this sample, the most likely target of an attack would be the reservoir. Thus, local police would work with reservoir personnel to ensure security of the water supply and focus efforts on determining any suspicious activities around the reservoir.

Secondary efforts would work with nuclear plant and airport personnel in a similar manner.

Once possible sources of threats and targets of threats are compiled, the **potential weapons** that might effectively be used against these targets by the sources can be compiled. Again, the weapons may be specific to the type of target and the type of terrorist group. Bombs might be used against buildings; chemical or biological weapons against a water or food supply. Also, remember to consider not only the weapons that might be used, but also the vehicles that might be used to convey the weapons.

The final inventory is of **pre-incident indicators**. Have previous threats or ideological communications been received from any of these groups? Have there been smaller incidents of disruption or disobedience that may lead up to violence? Has their been a build-up of funds, weaponry, or membership in the group? Is there any evidence that the group has been planning, staging, or gathering intelligence on targets? Are there any dates or incidents upcoming that might be marked by the group in some activity?

Some helpful information might be collected from various points. Transit hubs (airports, rail stations, and hotels) will tell us of movements in or out of group members. Informants might provide information on recent purchases of weapons. Self-store facilities might shed light on locations used to store material. Regulatory agencies such as departments of motor vehicles, tax authorities, or other licensing

groups may provide valuable data. Unusual events occurring on the streets may signal threatening activity. Patrol officers can be invaluable in collecting this level of information.

Commercial databases such as Lexis-Nexis and Choice Point are good sources of information on people and events. Private think-tanks and commercial strategic forecasting enterprises such as STRATFOR can also be helpful. Once material is gathered, it must be evaluated in keeping with the intelligence process. Both the reliability of the sources and the validity of the information should be quantified.[4] This quantification allows the analyst or officer to place greater (or lesser) value on the data and give it the proper weight when forecasting the potential acts to occur.

Risk Assessment Phase

More in-depth analysis occurs when the varied source materials are synthesized into a meaningful whole. While computerized information and databases may be of some help in the ordering of data, much of the products of the analytic phase may be written summaries of the information or matrices which might allow for comparisons. These overviews guide the collection of more information and the narrowing or hardening of the potential group or target.

When group profiles are assembled, for example, link charts showing the hierarchy of the organization may be appropriate. Timelines showing the history of the group may also be produced. Funding sources over time can be depicted in a commodity flow diagram. These visualizations assist us in seeing the overall picture. Once these products are completed, the actual risk assessment can be completed.

Key to determining the level of threat posed by extremist and terrorist groups is assessing the magnitude of threatened harm, the likelihood of occurrence, and the immediacy of the threat.[5]

One example of a threat assessment matrix used ratings of low, medium, and high to measure the threat level based on group evaluation characteristics, criminal predicate analysis, target analysis, and the consequences of intervention.[6]

In the local environment, each possible act could be scored and the scores compared to determine which possibilities are most likely or most threatening to public safety. For example, a county-level agency might be responsible for the security of government buildings, baseball parks, and the local water supply. Given equally strong sources of threats, the likelihood of greatest impact would be an attack on the water supply if a chemical or biological weapon were available.

It is important to note that "Consequence of Intervention" is part of the overall assessment model provided by Marynik. The actions taken by government agencies in response to a threat—whether they are sealing off a remote compound (such as the Branch Davidians in Waco), or bombing a foreign country (such as Afghanistan)—will generate a reaction on the part of the extremist or terrorist group, as well as a reaction from the public. These reactions must be taken into consideration when an action is considered.

Analysis is not complete unless and until conclusions are drawn and recommendations for action are made. The intelligence professional should develop hypotheses regarding what may occur and the likelihood of those hypotheses occurring. An analysis of the possible alternatives, as recommended by Heuer, is suggested. [7]

Intelligence gaps, clearly noted, can provide guidance for collectors and should be included in recommended actions.

Counter-measures that might be recommended could include evacuationing or relocating the target (if a person), limiting access to target (if a location), increasing short-term security and sustainable (longer term) security measures, increasing intelligence capability, implementing additional legislation, disseminating alert, creating a tip-line, offering a reward for information, etc.

In general, three levels of warnings may be disseminated: (1) advisories (broad, general threats; no immediate action needed), (2) alerts (cautionary information, may recommend change in posture or response), and (3) warnings (imminent or in-progress threats or attacks). [8]

Sharing Information Phase

Terrorism and extremism do not exist in a vacuum. These activities are often cross-jurisdictional and even cross-border. A terrorist threat or incident may occur locally, but the response is often multi-jurisdictional, and it is the responsibility of all agencies to notify the Federal Bureau of Investigation when a threat or incident occurs. [9]

While the local agency may collect and analyze data, the overall scheme is often only seen at a larger level; therefore, it is imperative that local operations perform a liaison role with involved state and federal agencies. This liaison should include two-way information sharing and keeping the local agency aware of events in other jurisdictions as well. This is important because, as noted by Fein and Vossekuil, "attackers and would-be attackers often consider multiple targets, who may live in different jurisdictions . . ." [10] A type of attack that is planned in one jurisdiction may also occur in a second or third, as witnessed by the use of commercial airlines to attack the World Trade Center in New York and the Pentagon in Virginia.

Sharing intelligence is often difficult within the territorial domain of law enforcement, but the greater goal of safety for all citizens should rise above this territorialism.

Analysis in Response to a Terroristic Threat or Act

Analysis is just as key in responding to terroristic acts as it is in helping prevent or deter terrorism. An actual terrorist or extremist attack is treated as a crime scene and thus the materials gathered can be analyzed to determine who perpetrated the attack and how. The range of information available (physical evidence, travel records, finances, surveillance data, written materials, etc.) would indicate a complex set of records to which analytic expertise should be applied.

Equally important is the ability of analysts to organize myriad leads and follow-up information collected by police officers or agents. While the individual officers may not be able to see trends or patterns in these bits of information, analysts usually can. Thus, subtle, yet important, trends may be identified by analysts.

If there has been a threat made, rather than a terroristic act, the general standard established at the federal level is to perform a threat credibility assessment. This includes their technical feasibility, operational practicality, and behavioral resolve. First, an assessment of the capacity of the threatening individual or organization to obtain or produce the weapon in question is done. Then, an assessment of the feasibility of delivering or employing the weapon in the manner threatened is completed. Finally, a psychological assessment of the likelihood that the subject will carry out the threat, including a review of any written or verbal statements by the subject is made. [11]

Caveats of Assessments

One reality of threat assessments is that perceived threats may be as powerful as real threats. This is never more true than in a terroristic situation in which the intent of the terrorist is to cause widespread fear. In other words, the threat may be actually felt by only a few but affect the minds of millions. Thus, while the threat may not be real, it cannot be ignored.

The impact of publicity is a two-edged sword. When publicity creates panic in the citizenry, this can be almost as damaging as a terroristic act. On the other hand, the knowledge of citizens can be of assistance to law enforcement when it is harnessed through a public awareness campaign.

Assessments should be completed by trained intelligence professionals. Training on intelligence and anti-terrorism should be sought. One source for pre-incident awareness training is the State and Local Anti-Terrorism Training (SLATT) provided by the Institute for Intergovernmental Research in cooperation with the Federal Bureau of Investigation. [12]

Assessments should also state what is not known. That is, if group members are suddenly missing or a location is abandoned and current locations are unknown, that is important. If a capability or a group's intent is not known, that should be stated.

Ongoing Commitment

The gathering and analysis of information relating to terrorism and extremism is not a one-time effort. The initial data must be updated regularly and with vigilance. Only through this type of commitment can we ensure that extremist and terrorist acts are prevented.

Bibliography

Departments of Justice, Defense, Energy, Health, Environmental Protection Agency, and Federal Emergency Management Agency. (2001, January). *U.S. Government*

Interagency Domestic Terrorism Concept of Operations Plan. Washington, DC: U.S. Government Printing Office.

Federal Bureau of Investigation. (2000). *Terrorism in the United States 1999.* Washington, DC: U.S. Government Printing Office.

Fein, R. A., & Vossekuil, B. (1998, July). *Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials*. Washington, DC: National Institute of Justice.

Heuer, R. J., Jr. (1999). *The psychology of intelligence analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

Marynik, J. (1998, April). *Threat assessment guide evaluating and analyzing criminal extremist groups*. Sacramento: California Department of Justice.

National Infrastructure Protection Center. (2001). Informational pamphlet. Washington, DC.

Peterson, M. B., Morehouse, B., & Wright, R. (2001). *Intelligence 2000: Revising the basic elements*. Lawrenceville, NJ: IALEIA and LEIU.

Marilyn B. Peterson is an analytic coordinator for the New Jersey Division of Criminal Justice and has 21 years of experience in local law enforcement. She heads the financial analysis function in the Division's money laundering section. She has also worked in white collar crime, narcotics, and organized crime.

She is a certified criminal analyst and is past president of the International Association of Law Enforcement Intelligence Analysts. She has written several books including *Applications in Criminal Analysis* (Greenwood, 1994; Praeger, 1998). Her most recent book is called *Intelligence 2000: Revising the Basic Elements* of which she was managing editor.

Her awards include several for written contributions to intelligence. She also has a Lifetime Achievement Award from the Society of Certified Criminal Analysts. She teaches basic, financial, and strategic analysis at state and federal levels.

Endnotes

[1] Intelligence, specifically, is the result of a process in which pieces of raw data are evaluated, compiled, and analyzed to determine their meaning.

[2] Federal Bureau of Investigation, 2000, pp. 3-13.

[3] The Federal Bureau of Investigation, for example, publishes reports on terrorism including both domestic and international groups which can be found on its website, <www.fbi.gov/publications/>. The U.S. Department of State also publishes *Patterns of Global Terrorism* at <www.state.gov/slct/rls/pgtrpt/2000/>.

A third source of information on terrorists and terror organizations is the U.S. Treasury Office of Foreign Asset Control at <www.ustreas.gov/ofac>. Updated lists of terrorists are published there.

[4] Reliability scales range from "A" (reliable) to "D" (reliability unknown), while validity scales range from "1" (confirmed) to "4" (cannot be judged). For more information on the evaluation process, see Peterson, Morehouse, and Wright, 2001.

[5] Marynik, 1998, p. 12.

[6] Ibid., p. 23.

[7] Heuer, 1999, p. 101

[8] Informational Pamphlet, National Infrastructure Protection Center, 2001, p. 3.

[9] Departments of Justice, Defense, Health, Energy, et al., 2001, p. 27.

[10] Fein and Vossekuil, 1998, p. 31.

[11] Departments of Justice, et al., 2001, p. 27.

[12] Further information can be found at <www.iir.com/slatt/training.htm>.

Local Law Enforcement's Role in Preventing and Responding to Terrorism

Gerard Murphy, Senior Research Associate
Martha Plotkin, Director of Legislative Affairs
David Edelson, Assistant Director of Communications

Introduction

The nation is embarking upon a new and vigorous fight against terrorism, and local police agencies must be full partners in these efforts. While local law enforcement has always had a role in first response and critical incident management, they will be asked for the first time to assume new and uncertain responsibilities. They welcome this challenge and believe they can make a valuable contribution to the nation's anti-terrorism efforts; however, they cannot assume these responsibilities without significant federal support.

The Police Executive Research Forum (PERF) is a national nonprofit organization of progressive police executives who collectively serve more than half of the nation's population. PERF members have long supported the expansion of wiretap authority and other surveillance authority that keeps pace with new technology; we choose to focus, however, on local needs that may not be adequately emphasized in current federal proposals. Indeed, PERF members, such as PERF Legislative Chair Chief Ed Flynn of Arlington County, Virginia, whose officers were the first responders to the Pentagon, have unique insight into the role that local police can play. This article presents the results of a preliminary survey of local police chiefs regarding their roles, needs, and recommendations for contributing to the fight against terrorism. Proposed responses include such measures as best practices in local police preparedness, model policies and protocols, and local and federal cooperation models that address existing intelligence sharing obstacles.

PERF Survey

PERF recently surveyed more than 250 police chiefs from large jurisdictions on their respective needs and capabilities in addressing domestic terrorism. PERF members were and will continue to be agents of prevention and first responders to acts of terrorism within the United States, and PERF wanted to get a quick assessment of their needs to better prevent and respond to terrorist acts. Within 48 hours, more than 150 chiefs responded that their greatest needs were for funding, intelligence gathering and sharing, equipment and technology, and gaining access to information from federal agencies. They reported that they were most prepared to coordinate with neighboring police agencies, engage in critical incident management, coordinate with non-police agencies, and develop written policies and plans for anti-terrorist efforts. Fifty-nine percent of the responding agencies have federal facilities in their jurisdictions, with 52% having commercial airports. Thirty-nine percent reported having a military installation in their jurisdiction.

The preliminary survey results have confirmed what we all suspected—that local police have a significant role in responding to critical incidents, stabilizing the community after an incident, sharing information with other police agencies, and establishing multi-agency task forces. The survey revealed for the first time that local police believe their role in fighting terrorism is expanding and that they welcome this change. In particular, they believe they can make a valuable contribution to preventing terrorism, by building on their community policing networks to exchange information with citizens and gather intelligence.

Respondents indicated, however, that they needed more information and training on the nature, dynamics, and operations of international terrorism and needed to be more prepared. Most responding agencies reported that they would rely on more general critical incident plans—with only 16% indicating that they would rely on a terrorist incident plan. This also may reflect the absence of such specific plans. More than 75% of the respondents have no anti-terrorist unit. The remainder have either a formal, but part-time, anti-terrorism function or a full-time unit.

More than 30% of the agencies reported participation in existing multi-jurisdictional anti-terrorist task forces involving local, state, and federal agencies. The vast majority of responding agencies were aware of intelligence, equipment, training, and technical assistance resources for terrorism preparedness. Far fewer were aware of model policies, programs, or adequate financial assistance.

The areas in which responding police agencies said they wanted or needed additional training or assistance was (in order of greatest concern) intelligence gathering capabilities, acquiring and using equipment or technology, and accessing external funds. In the comment sections of the surveys, the overwhelming majority of respondents expressed concern that federal authorities do not adequately share intelligence information. PERF members proposed that local police support should include developing "best practices" model policies and protocols, technical assistance, and training for increased preparedness.

Based on the preliminary survey results and discussions with many of PERF's members, the following outline and information were developed to help ensure that local law enforcement needs are appropriately and adequately addressed by policymakers.

A. Local police agencies have critical roles to play in preventing and responding to terrorism.

1. Prevention

- Federal law enforcement cannot do it alone.
- Local police can and will play a critical role in **gathering intelligence** on suspected terrorists and knowing what to do with that information. Many have critical information about individuals living in their communities.
- Local police agencies are uniquely qualified to assess **community concerns and fears** that are critical to effective intelligence gathering. This is especially true in light of the effects and progress of **community policing**

and its emphasis on citizen engagement, partnerships, trust, information sharing, and collaborative problem solving.

- Local police can be used effectively to prevent terrorism if they **exchange intelligence** information with other local, state, and federal agencies and are trusted to maintain the confidentiality of sensitive information.

- Police can and must play a critical role in other aspects of terrorist prevention, such as identifying, assessing, and reducing threats to local targets.

2. Critical Incident Prevention, Preparations, and Response

- Clearly, local police play a key role in preventing, preparing for, and responding to terrorist attacks. They can provide important early warning systems and critical evacuation, emergency medical, and security functions.

- Local police will have an increased role in developing and implementing **local critical incident plans** that consider many forms of terrorist attacks.

- Local police agencies will have to work with county, state, and federal law enforcement and general government officials to plan and implement **coordinated critical incident management plans** that ensure the effective management of a terrorism scene.

3. Aftermath

- Local police agencies will have responsibility for working with communities and local leaders to **stabilize communities** traumatized by terrorist attacks. Local police play a crucial role in reducing fear, as well as preventing and responding to hate crimes and bomb threats.

- **Citizen fear** of additional attacks and unknown consequences will cause communities to look to local law enforcement for answers and reassurance about potential terrorist threats.

- In the event of a terrorist attack, communities will place inordinate demands on local police agencies for information, services, and other assistance. These agencies will have to meet the needs of citizens and other stakeholders, even while they respond to the scene of a terrorist attack.

B. Local police agencies need assistance in assuming these critical roles and implementing new relationships, policies, and procedures.

1. Coordination Strategies

- There is a need to develop strategies for local police agencies to collaborate with surrounding law enforcement officials (local, state, and federal) for preventing, preparing for, and responding to terrorism. Local police

must be equal partners in any collaborative efforts if those strategies are to be effective.

- Local police need assistance in coordinating with non-police agencies (e.g., fire, EMS, 911, FAA, health, hazmat, etc.). This will require much improved interoperability for communications systems and strategies for developing effective emergency operations centers.

- Local police agencies need to determine the nature of their role in the new U.S. Attorney-led task forces. Local, state, and federal agencies need to develop protocols for improved sharing of intelligence and information to make these task forces effective. Local police chiefs expressed concern with getting intelligence and information from some federal agencies even when they provided intelligence and other support to those federal agencies. (Some chiefs have proposed that local law enforcement executives may need to get adequate security clearances to facilitate information sharing when an incident arises.) Information exchange issues are complex but must be remedied. The exchange of information between locals and the FBI, FAA, FEMA, and others has been plagued by uneven responses that are largely dependent on individual personalities and willingness to share. Issues of mutual trust must be addressed, and guidelines for protecting sensitive information must be established.

- Local law enforcement personnel need models for coordinating with other law enforcement agencies (e.g., federal agencies, other municipal/sheriff, transportation, state) that will allow for the exchange of intelligence (e.g., the timely sharing of "watch list" suspects with identifying information on NCIC), crime analysis, emergency communications, and risk assessment information. Successful collaboration and information sharing programs exist and could serve as models for anti-terrorism task forces. Existing anti-terrorist task forces should be evaluated and integrated into new federal initiatives.

- A federal office could coordinate the development of models and protocols either directly or through a contractor by compiling information and convening experts from around the nation to develop these models and protocols. Those sessions could include discussions and steps to alleviate obstacles to local-federal cooperation. A detailed survey could be used to identify "best practices" around the nation, and this information could be fed to a task force comprised of local law enforcement leaders, as well as representatives from other law enforcement agencies (e.g., federal agencies) for distribution.

- A federal office could assist with the development of regional task forces (especially those involving just local agencies) by providing experts to assist in the needs assessments, project planning, and training efforts. Existing anti-terrorist task forces, High Intensity Drug Trafficking Area (HIDTA) task forces, and regional crime analysis information systems provide many examples of effective collaboration. Any federal initiative must build on the expertise and existing networks to reduce redundancy and provide the broadest foundation for information sharing.

2. Policies/Procedures

- Local police agencies will need assistance in developing sound written policies and plans related to investigations, intelligence gathering, and information analysis, as well as mutual aid agreements and memoranda of understanding with those agencies with which they plan to form task forces. This would include task forces with federal agencies but could also include regional task forces initiated on the local level.

- Local and federal agencies need to develop protocols that allocate the responsibilities and coordinate managing a critical incident scene (perimeter, search, rescue, recovery, etc.) with the need to initiate the immediate follow-up investigation. For example, at the Pentagon, local and federal agencies faced conflicting priorities about managing the scene. Local and federal agencies need to develop much better detailed protocols that facilitate intelligence exchanges while also maintaining the confidentiality of the information and sources.

- Following the processes outlined above, a federal office or its contractor could develop a report that outlines the essential components of regional task forces and describes content that could be customized to each agency.

- A federal office could assist with the development of local or state initiated task forces by providing technical assistance to agencies as they tailor the model policies/procedures to their own jurisdictional situation. The PERF survey revealed that more than 45 local agencies have initiated formal discussions to form anti-terrorist task forces.

3. Equipment and Technology

- Local police agencies will need technology, equipment, and computer resources for advanced intelligence gathering, analysis, and sharing with other law enforcement agencies. This type of equipment and technology goes well beyond the equipment routinely distributed to local agencies through federal disaster preparedness efforts.

- Local police agencies need new and additional equipment, to enhance their ability to prepare for and respond to a critical incident. Interoperability of communications is a critical issue, as was aptly demonstrated at the Pentagon. Arlington County incident commanders could not communicate with other responding agencies that did not have similar radio equipment. Cellular communications are essential to an effective public safety response; however, peak use of cellular technologies caused communications networks to overload and fail, leaving public safety agencies without cellular communications.

- A federal office could disseminate funds directly to agencies for technology and equipment to enhance intelligence-gathering capabilities and to manage a disaster scene. Most jurisdictions do not have the resources, technology, and equipment that were available to local police serving the

Pentagon and World Trade Center. Those needs increase dramatically when nonconventional weapons are used.

4. Training

Local agencies need training and education in the following:

- Understanding the nature, dynamics, and operations of international terrorist groups that may operate in/against the United States and how that translates into more effective patrol and investigative functions
- Understanding the locations, movements, and plans of international terrorist cells that live, work, and assimilate in local communities
- Conducting inquiries and investigations into potential terrorists while safeguarding the constitutional rights of all people in the United States.
- Gathering and analyzing intelligence on potential terrorist activities
- Conducting threat assessments
- Managing critical incidents; applying incident command protocols to managing critical incidents
- Conducting post-incident investigations
- Providing post-incident crisis debriefing and management for service providers and citizens
- Coordinating the development of model curriculum for inservice and specialized training and coordinating train-the-trainer sessions

5. Democratic Policing

- Police need assistance in dealing with the issue of racially biased policing that could manifest itself in new ways as a result of the recent terrorist attacks.
- A federal office could promote the dissemination/accessibility of all racially biased policing and hate crime resources and coordinate the development of supplemental reports focusing on the issue particularly as it pertains to terrorism.
- A federal office could coordinate the development of the academy and inservice training and community education programs strongly recommended in the COPS-funded report on racially biased policing—tailored to include the new manifestation of bias following the terrorist attacks.

C. The COPS office is the federal agency best suited to coordinate the efforts that will enable local law enforcement to assume and fulfill their roles. The COPS office . . .

- Has ongoing credible relationships and positive working history with local police agencies.
- Has an innovative and responsive grant making and training infrastructure that was developed specifically to meet the needs of local law enforcement.
- Has the oversight mechanisms in place to monitor local law enforcement.
- Has a history of providing a timely response to local law enforcement.
- Knows best how the strengths of local police agencies—particularly in this age of community policing—can best be applied to respond to this problem.
- Has the capacity to quickly convene law enforcement practitioners to focus on emerging issues.

Gerard R. Murphy, senior research associate, joined PERF in September 2001 with 20 years experience in law enforcement. Most recently, Murphy was the Director of Planning and Research for the Baltimore County Police Department. His primary responsibilities included developing and implementing the department's strategic plan, researching and developing all department policies, managing over $20 million in state and federal grants, and serving as the agency's accreditation manager. Prior to holding that position for four years, he was the assistant to the police chief for eight years. In that capacity, he worked for three different chiefs, providing policy advice and guidance and undertaking a variety of special projects to improve organizational efficiency. In addition, during his entire tenure with the department, he served as the executive director of the Baltimore County Police Foundation, a philanthropic organization of over 20 corporations that provide guidance, resources, and recognition to the police department.

Before joining Baltimore County, Murphy was an assistant professor of public affairs and a research associate at PERF from 1981 to 1989. While at PERF, he played a key role in helping to develop CALEA, writing standards and designing the on-site assessment process. He also helped to launch PERF's management services function. Most notably, Murphy completed the initial research and development for improving the police response to persons with mental disabilities.

Murphy holds a master's degree in public policy, has completed extensive work towards his doctorate in public policy, and is a graduate of the Federal Executive Institute.

Martha R. Plotkin, director of communications and legislative affairs, has been with PERF for more than 15 years. She currently directs PERF's publications, media, and legislative programs. An attorney, Plotkin also works on amicus briefs and other legal issues affecting police agencies. She is the author of *A Time for Dignity* and other articles and training materials on the police response to elder abuse. She is coauthor of *Police and the Homeless: A Status Report*, and editor of *Under Fire: Gun Buy-Backs, Exchanges, and Amnesty Programs*. She has managed and continues to contribute to research projects on the police response to special populations and victims. Ms. Plotkin completed the legal studies program at Brandeis University where she received her BA in psychology. She earned her law degree from the George Washington University Law School.

David Edelson, assistant director of communications, joined PERF in March 2001. He is the editor of PERF's newsletter, *Subject to Debate*, works on editing and production of PERF books and marketing materials, and assists with media relations.

Prior to joining PERF, David worked as a public affairs representative at the American College of Physicians–American Society of Internal Medicine (ACP-ASIM). In college, he worked for three years as a reporter and editor at *The Daily Collegian* and interned with the press offices of the New York State Attorney General and the New York Giants. He earned his BA degree in journalism from Penn State in May of 2000.

Illinois Sheriffs, Police Chiefs Seek More Collaboration, Cooperation After September 11

Robin A. Johnson

The terrorist attacks of September 11 are producing far-reaching consequences for local public safety services. Increased demand for security measures is straining the capacity of local law enforcement budgets as the economy continues to decline, lowering revenues available to cities and counties. Sheriffs and police chiefs are caught in a vise in that they are trying to balance demands for additional services while remaining fiscally responsible.

This confluence of events since September 11 has resulted in calls for more cooperation among law enforcement agencies. Internal cooperative agreements between local government agencies, such as police and fire departments and between local governments, such as municipal police departments and county sheriffs' offices, are ways to share resources, avoid duplication of services, save tax dollars, and most importantly, enhance homeland security.

In Illinois, which has a fragmented system of local government, some cities and counties have cooperative agreements for public safety services in place. Some have consolidated certain services, and many contract for services with other law enforcement agencies. Existing cooperative agreements provide a solid foundation for further regional efforts among local law enforcement agencies.

This article will examine the extent of cooperation among local law enforcement agencies in Illinois based on surveys of police chiefs and sheriffs. Some examples of cooperation are included to highlight the ways local officials are collaborating. First, it is useful to provide an overview of the issue from a national perspective.

National Trends

After the terrorist attacks in New York City on September 11, local police, fire, and emergency response teams mobilized in a coordinated fashion that "will be a lesson" to other local governments in the region, according to Harlan Cleveland, a former national security official.[1] Problems occurred, however, as the agencies found it difficult to communicate by radio because they operated on different frequencies. A similar problem occurred in response to the Oklahoma City bombing in 1993.

As a result of limited collaboration, inadequate training, and the changing nature of terrorist acts, city officials nationwide are mobilizing local resources to ensure public safety, secure public facilities, and enhance the response capabilities of their communities. For example, a survey of cities conducted by the National League of Cities (NLC) found that 73% of responding officials said they plan to update or revise their emergency plans, and 52% reported that they are seeking anti-terrorism training and increasing security for public buildings (see Table 1).[2] The survey found that large cities (more than 100,000) are significantly more likely to report these findings than smaller communities.

Table 1. Measures Taken or Planned by Cities in the Aftermath of September 11

Measure	Percentage
Revision of emergency plans	73
Increased interdepartmental cooperation	67
Increased intergovernmental cooperation	64
Increased water security	61
Additional anti-terrorism training	52
Increased government building security	52
Increased public event security	47
Conduction of emergency response exercises	45
Increased nongovernmental cooperation	42
Increased public health cooperation	42
Acquisition of more emergency equipment	34

Source: *Nation's Cities Weekly*, October 22, 2001

City officials are also increasing the amount of interdepartmental and intergovernmental cooperation. For example, 67% of responding cities are increasing interdepartmental cooperation and coordination, and 64% are increasing intergovernmental collaboration, the second and third highest rated measures being planned by cities in the survey.[3] In addition, 42% of city officials report they plan to increase coordination with nongovernmental agencies and public health and medical facilities.

A different post-September 11 survey of city officials conducted by the NLC found that many city leaders support more regional cooperation among local governments as a way to meet increased public safety costs with fewer revenues.[4] Most city officials also called for the state and federal governments to help facilitate regional and intergovernmental cooperative efforts and assist with and help fund enhanced training for local law enforcement agencies. Illinois responded by planning regional meetings throughout the state designed to help plan for better coordination of public safety efforts in the future.

Trends in Illinois

Illinois has more local governments than any other state in the nation[5] and, therefore, tremendous potential for greater local law enforcement collaboration. With so many local governments in Illinois offering similar services, there are ample opportunities for consolidation and reducing duplication of effort. Municipalities and counties both provide similar law enforcement services. Each entity has its own personnel, vehicles, facilities, and equipment. Increased efficiency can also occur when adjacent or overlapping governing bodies consolidate service delivery.

Greater cooperation in Illinois local law enforcement is being driven by the need for enhanced security and declining financial conditions. Many local governments were experiencing fiscal difficulties prior to September 11; since then, economic conditions have deteriorated further, forcing many local governments to consider budget reductions and revenue enhancements.

Public safety services are labor intensive and are the largest expenditure category in Illinois' local government budgets.[6] Therefore, any attempts to reduce spending in cities and counties usually involve cuts in police and sheriffs' budgets. For example, in response to a five percent across-the-board spending cut among county agencies, Peoria County Sheriff Chuck Schofield estimated a reduction of approximately $600,000 and layoffs of 18 employees.[7] Discussions of budget cuts and fewer deputies are occurring as the county is now providing more patrol and security services since September 11. Other counties, such as Knox and Woodford, are also dealing with budgetary shortfalls and are asking sheriffs' departments to reduce expenditures, which involves lowering staffing levels.

As fiscal conditions worsen in local governments across the state and demands for heightened security increase, opportunities for collaboration and cooperation take on added importance. Many local law enforcement agencies have begun meeting to better coordinate their efforts. For example, Peoria County held a meeting that included 20 representatives from local police, fire, health, and military agencies.[8] The meeting was the first in a series designed to prepare the county and local agencies to respond to a biological or chemical attack until additional resources could arrive.

Some information exists on the extent of cooperative efforts in Illinois local law enforcement agencies. The Illinois Law Enforcement Training and Standards Board, working in cooperation with the Illinois Law Enforcement Executive Institute, Illinois Institute for Rural Affairs at Western Illinois University, the Illinois Sheriff's Association, and the Illinois Association of Chiefs of Police, surveyed municipal police chiefs and county sheriffs on a variety of issues in recent years.

Survey Results: Consolidation

A 2000 survey of 78 Illinois sheriffs listed four types of services that sheriffs could consolidate with other local governments.[9] None of the services received a majority of support for consolidation among responding sheriffs. The service sheriffs favored for consolidation most often is 911 communications systems by 35.5% of respondents (see Table 2). 911 systems are becoming more expensive due to the cost of advanced telecommunications equipment. A majority (60%) of northern Illinois sheriffs support consolidated 911 systems—the only subgroup that gave majority support for any consolidated service. Some 911 systems already involve multiple jurisdictions.

Table 2. Sheriff's Support for Consolidated Services

Service	Percentage
For 911 communications systems	35.8
With municipalities within the county	29.4
Consolidated city/county facility	17.9

Source: ILEEI/IIRA, Survey of County Sheriffs, 2000

One reason many sheriffs favor consolidation of 911 services is that most departments already have cooperative agreements with other entities for dispatching services. Approximately three-fourths (75.6%) of sheriffs statewide dispatch for other law enforcement agencies, and 70.5% dispatch for area fire departments (see Table 3). Also, 67.9% report that their departments also provide dispatching for ambulance services and 55.1% for emergency medical technicians (EMTs).

Table 3. Extent of County Dispatching for Other Law Enforcement Agencies

Agency	Percentage
Other law enforcement	75.6
Fire departments	70.5
Ambulance	67.9
Emergency medical technicians (EMTs)	55.1

Source: ILEEI/IIRA, Survey of County Sheriffs, 2000

Information on collaboration among municipal police chiefs in Illinois is from a 1996 survey of 642 chiefs.[10] Police chiefs currently collaborate on 911 services most often, as reported by one-third (33.3%) of respondents (see Table 4). A slightly larger number of police chiefs (35.6%) favor a regional approach to 911 services. Thus, more than two-thirds of police chiefs (68.9%) either have cooperative 911 communications systems in place or support them for the future.

Table 4. Municipal Consolidation of Services

Extent of Consolidation of Services in Cities

Service	Percentage
For 911 communications systems	30.8
With county agencies	17.9
With municipalities within the county	17.9
Consolidated city/county facility	12.8

Police Chief's Support for Consolidated Services

Service	Percentage
For 911 communications systems	34.1
With county agencies	27.3
With municipalities within the county	13.6
Consolidated city/county facility	9.1

Source: ILEEI/IIRA, Survey of Municipal Police, 1996

Sheriffs' departments could also consolidate some services with municipalities within the county. If cities or towns have existing inhouse police departments, it could be more cost effective to merge operations. This option has not been implemented in Illinois although some counties and cities in other states have merged to create a consolidated law enforcement agency.

In the survey, 29.2% of sheriffs said that they favored consolidation of services with area municipalities. It is assumed that the sheriffs would have operational control over a consolidated force since the county has the larger jurisdictional boundary; therefore, it is somewhat surprising that more sheriffs are not in favor of a joint city-county police force. Perhaps sheriffs know the political realities of gaining support for and implementing a merger and simply do not believe it is realistic.

In results similar to the survey of county sheriffs, few police chiefs expressed an interest in cooperative or regional delivery of services with counties. Only 16 police chiefs (15.7%) reported that they provided services jointly with counties, and nearly one-fourth (23.1%) of them said that they were interested in pursuing regional agreements with counties.

Fewer sheriffs (17.8%) favor a consolidated county/city facility. This could be an attractive option for some because it stops short of consolidating services but combines departments in a single facility that could improve communications and planning. McDonough County/Macomb and Winnebago County/Rockford share public safety buildings and jail facilities.

Only 11.8% of police chiefs report having consolidated city/county facilities, and 7.7% favor a combined facility. It is somewhat surprising that less than one in five police chiefs (19.5%) have combined facilities in place or favor them. Perhaps police chiefs believe that control over such facilities would belong to the sheriff's office.

Few police departments (18.3%) said that services were provided in conjunction with other municipalities. Cooperative agreements among cities depend on close proximity, making these agreements more likely in suburban areas than in rural counties. Nineteen police chiefs said that they would favor some form of cooperation with other cities. The same number said that they currently had such arrangements in place. Overall, 36.3% of police chiefs collaborate with other municipal departments or support such efforts.

Interestingly, the percentages of support for consolidation among sheriffs changed very little since 1995 when a similar survey of sheriffs was conducted. This is surprising in that some turnover likely occurred among sheriffs in the 1998 general election, which featured contests for the office across the state. Presumably, more sheriffs will be interested as more successful partnerships occur. For now, consolidation may look good on paper, but the idea has not won over many sheriffs yet in Illinois.

Survey Results: Intergovernmental Relations

Because crime knows no boundaries and criminals can pass through multiple jurisdictions, it is important for sheriffs to have good working relationships with other law enforcement agencies. Smaller sheriffs' departments especially rely

upon other larger law enforcement agencies with more resources to assist in more sophisticated and technical cases.

There are many examples of law enforcement agencies working together and sharing resources. Multi-county drug task forces involve sheriffs' offices and municipal police departments working together to combat the sale and possession of illegal drugs. Agencies also have mutual aid agreements that provide additional support in cases where more manpower and/or equipment is needed.

While the amount of consolidation of services is limited, most sheriffs report good working relationships with other law enforcement agencies, which provides a basis for future cooperative efforts. (This question was not asked on the survey of municipal police chiefs). More than 80% of sheriffs rate relations with the Illinois Department of Law Enforcement as good with 37.2% rating them as highly favorable and 44.9% as favorable (see Table 5). Only two sheriffs said relations were unfavorable, and one said highly unfavorable.

Table 5. Sheriffs' Relationships with Other Law Enforcement Agencies

With the Illinois Department of Law Enforcement

Rating	Percentage
Highly favorable	37.2
Favorable	44.9
No opinion	14.1
Unfavorable	2.6
Highly unfavorable	1.3

With Municipal Police Departments

Rating	Percentage
Highly favorable	48.7
Favorable	50.0
No opinion	1.3
Unfavorable	0.0
Highly unfavorable	0.0

Source: ILEEI/IIRA, Survey of County Sheriffs, 2000

Relations with municipal police departments are even better. All sheriffs except one had a favorable opinion with 48.7% reporting that the relationship is highly favorable and 50% saying it is favorable. Thus, no sheriffs have unfavorable relationships with municipal police departments in their areas.

Case Study: Monmouth, IL

Local law enforcement officials with cooperative arrangements in place before September 11 have the foundation in place to expand those efforts to include homeland security and anti-terrorism functions. For example, Monmouth Police Chief Gary Morefield developed several initiatives since his appointment in 2000 that involve expanded internal training, interdepartmental cooperation, and intergovernmental agreements.

First, Morefield allocated departmental funds and state grant funding for advanced training for Monmouth's police officers and purchasing tactical equipment. Twelve police officers in the department have received advanced tactical training designed for responding to shootings, school-based incidents, or other emergency situations. In addition, one officer is trained as a hostage negotiator and two are trained as snipers.

Morefield also involved the city's fire department in emergency response measures. Three city firefighters received tactical and paramedic training and are included in the city's tactical team. The agreement was developed by Morefield and Fire Chief Mark Gladfelter through a letter of understanding. Inclusion of firefighters with paramedic training on the tactical team ensures that injured victims receive the earliest possible medical attention and transport.

Finally, Morefield developed a countywide narcotics task force in conjunction with Warren County Sheriff Richard "Floaty" Hart. The sheriff's department trained two deputies as tactical officers, one as a sniper, and one as a hostage negotiator. Under an agreement worked out between the local governments, city police officers were deputized to allow them to pursue incidents beyond the city's boundaries. While the task force and supporting measures were developed to fight narcotics, Chief Morefield and Sheriff Hart plan to expand the scope of cooperative activities to include anti-terrorism efforts.

Since September 11, Chief Morefield has begun working in partnership with the local hospital to develop a bio-terrorism policy in response to an anthrax-related incident in October 2001. Morefield is involving the police department in an expanded collaboration with the fire department regarding hazardous materials (HAZMAT) training. The Monmouth chief is also participating in state-sponsored regional meetings designed to inform and train local public safety agencies on the threat of terrorism.

Chief Morefield believes that the expanded interdepartmental and intergovernmental cooperation the city is pursuing since September 11 would be more difficult and time-consuming without the existing foundation in place. As regional approaches to public safety issues become more common, cities like Monmouth with prior experience in cooperative agreements will be well positioned to enhance their community's security and respond better to emerging threats to public safety.

Conclusion

The events of September 11 have dramatically changed the day-to-day administration and priorities of public safety agencies in the Untied States. Demands for greater security measures and emergency responses to terrorist acts place an added burden on already strained local resources. The need for expanded services and an economic downturn that has slowed local revenues have combined to place a greater emphasis on regional and cooperative approaches to public safety issues.

In Illinois, the amount of cooperation and coordination among local public safety agencies was somewhat limited prior to September 11. Some municipal police agencies and sheriff's departments had contracted services with other public safety agencies and participated in intergovernmental agreements such as for 911 communications. Others, such as Monmouth, had moved beyond traditional cooperative approaches and implemented several innovative interdepartmental and intergovernmental strategies.

The move towards greater collaboration among public safety agencies is welcome and long overdue. While cooperation has traditionally been driven by a desire to share resources to enable more efficient delivery of services, the reasons have broadened beyond efficiency to include an expanded scope of services, including anti-terrorism. Current efforts underway to increase collaboration may lead to a new era of regional cooperation that will enhance public safety and ensure more efficiency in the way those services are provided to citizens.

Endnotes

[1] Peirce, N. (2001, September 21). Collaboration a matter of life, death. *Peoria Journal Star*, p. A5.

[2] Hoene, C. (2001, October 22). Cities increase security, coordination: Worry about economy. *Nation's Cities Weekly*, p. 1.

[3] Ibid.

[4] Hoene, C. (2001, October 1). Cities mobilize public safety resources, worry about costs. *Nation's Cities Weekly*, p. 3.

[5] Office of the Comptroller. (2000, October). Local government in Illinois. *Fiscal Focus Quarterly*, p. 1.

[6] Ibid, p. 9.

[7] Peoria county budget leaves few choices [Editorial]. (2001, October 28). *Peoria Journal Star*, p. A4.

[8] Kravetz, A. (2001, October 13). Peoria rushes to plan for attack. *Peoria Journal Star*, p. B1.

[9] Johnson, R. A., Campbell, R. K., & Walzer, N. (2001). *Illinois sheriffs' departments: Trends and concerns*. Macomb: Illinois Institute for Rural Affairs.

[10] Hazlett, M. H., Fischer, R., York, L., & Walzer, N. (1998). *Municipal police departments: Trends and concerns*. Macomb: Illinois Institute for Rural Affairs.

Robin A. Johnson is a governmental relations consultant based in Monmouth, IL and author of *Small Town Policing in the New Millennium: Strategies, Options, and Alternate Methods*. He previously served as director of the Illinois Center for Competitive Government and as director of the Privatization Center for the Reason Public Policy Institute. Johnson has a BA from Monmouth College and an MA from Western Illinois University. He is a former alderman in Monmouth and served on the Public Safety Committee.

Homeland Defense Training

Elliot Spector

Major impediments currently exist that are inhibiting our ability to engage in an effective homeland defense and war against terrorism. The first is that our local and state law enforcement officers are unprepared and inadequately trained to engage in the effort. Secondly, there is disconnection between the local and federal law enforcement agencies, inhibiting the proper channeling of information and appropriate cooperative effort. It is comforting that our government officials have nationally put our law enforcement officers on heightened alert. Unfortunately, these officers, for the most part, have no idea what heightened alert is, do not know how to recognize a potential terrorist or terrorist act, do not know how to deal with a suspected illegal alien, do not know how to gather intelligence or investigate suspected terrorists or terrorist activities, and do not know how to recognize weapons of mass destruction or how to respond to a suspected terrorist act.

Do We Need Local and State Law Enforcement Officers to Play a Role in the War on Terrorism?

President Bush, Governor Ridge, and all of our government leaders recognize that local and state law enforcement is an integral part of our homeland defense. They undoubtedly recognize the reality that although the marines can deploy to a terrorist act, the police will be there hours earlier. Although the FBI is best able to collect and evaluate intelligence, the average citizen may more frequently speak to their local law enforcement officer. Most importantly, it is the everyday, on-the-street officer who will likely first come in contact with terrorists long before a terrorist act. As a perfect example, Timothy McVeigh was detected during a normal motor vehicle stop. Everyday, wanted criminals are discovered during chance encounters. Some of the terrorists of September 11 had contact with law enforcement officers, weeks and months before that tragic day. Undoubtedly, the terrorists planning tomorrow's destructive acts are living in our neighborhoods, traveling our roads, and having contact with local law enforcement on a frequent basis.

The 500,000 plus law enforcement officers who are in daily contact with millions of private security officers and citizens, can serve as the foot soldiers for our federal agencies but only if they are properly trained. The need for this training goes beyond the fear that unnecessary terrorist acts will occur because we were unprepared or they go undetected. The fragile sense of security offered by our national leaders bolstered by the "law enforcement alert" will deteriorate quickly if our 500,000 officers begin to inform our citizenry that the alert is a fiction.

The Plan

The objective of the National Homeland Defense Training Plan is to provide the best quality training in the most efficient and economical way possible. The goal is to create a system for a national, unified effort to eliminate the terrorist threat. The linchpin of the project is to create liaisons within our local and state law enforcement agencies to work as intermediaries between our federal agencies and their own departments and communities.

National Law Enforcement Anti-Terrorist Training/Liaison Program

Goals

1. Train-the-Trainer Programs

Training trainers is the most effective and efficient way to educate the law enforcement community. Anti-terrorist training experts and materials are immediately available to meet this need. What is now needed is a focused and coordinated effort to condense existing training into a nuts-and-bolts curriculum and to provide relevant materials to trainers who can in turn bring this information back to their communities. Realistically, a minimum of 1000 trainers can be taught in the first month, and they in turn could train 100 to 200 officers in their departments/regions thus providing training to potentially 100,000 to 200,000 officers within 60 days. Within six months, initial basic training could be provided to all law enforcement officers in our nation.

2. Anti-Terrorist Liaison

It is crucial that an effective channel of communication exists between state and municipal law enforcement agencies and federal authorities. The anti-terrorist trainer could fulfill this need. Federal authorities wishing to disseminate general information, update training, or provide specific information to a locality will have a trained and competent person to turn to. In turn, when intelligence is gathered in particular localities, a liaison trained in how to screen and evaluate such information could effectively channel it to the appropriate federal agency.

3. Time-Line Goals

Day 1
- Program approval
- Selection of curriculum facilitator
- Selection of program administrator

Day 5
- Begin distribution of program notice and registration.

Day 20
- Complete curriculum and selection of instructors.
- Begin preparation of materials, training needs, and equipment.

Day 45
- Class One – Minimum goal: 250 students, divided into five groups

4. Potential Basic Curriculum:

I. Recognizing and identifying terrorists and terrorist activities

A. Characteristics of terrorist and terrorist activities

B. Resources available for verifying suspected terrorists and terrorist activities

C. Recognizing bombs and weapons of mass destruction

II. Related legal issues

A. Legal standards related to potential contacts with terrorists and actions which may be taken when confronted by potential terrorists and aliens under circumstances not amounting to reasonable suspicion

B. Legal authority for stopping and detaining suspected terrorists and aliens

C. Search issues regarding reasonable suspicion or probable cause when searching potential terrorists, vehicles, or premises

D. Investigation techniques, questioning, and interrogation issues

III. Intelligence gathering

A. What to look for and what to ask

B. How to screen and evaluate information

C. Who to contact with potential valuable information

D. Resources available to maintain current information on terrorists and terrorist activities

E. Disseminating information to law enforcement administrators, supervisors and field officers, private security, and the community

IV. Reacting to terrorist attacks

A. Role of law enforcement administrators, officers, and emergency response/SWAT teams

B. Evacuation and rescue plans

C. Emergency contacts and resources

D. Developing relationships and coordinating efforts with fire; rescue; and other local, state, and federal agencies

V. Homeland security

A. Security of potential targets

B. Developing citizen awareness and cooperation

C. Deterring terrorist acts

Consolidating Training Resources and Other Programs

By providing training at a single site, training groups and trainers could rotate to provide the maximum amount of training for a large number of individuals in a condensed time. Also, by consolidating training resources, such resources could be utilized efficiently and economically by large numbers of groups.

In addition to law enforcement training, specialized train-the-trainer programs should be developed for . . .

- Airport security
- Sensitive facility security
- Airline crews
- Fire and rescue personnel

Federal Program Vs. Local/State Programs

The federal government will make available to local and state entities hundreds of millions of dollars to fight the war on terrorism. Unfortunately, the feeding frenzy at this "pork barrel" will interfere with our nation's ability to effectively get the job done. Historically, egos and need to control have prevented progressive law enforcement initiatives. If there was ever a time to put aside egos and desire for control, this is it. A bit of honest introspection should convince local and state law enforcement officials that a federal plan is clearly the better option. They should ask themselves the following:

1. Do I, or any of my officers, know more about terrorism, how to seek out terrorists, how to recognize terrorist acts, how to protect the community against terrorism, than our federal agency terrorist experts?

2. Can I put together a comprehensive plan that can ensure a better national unified effort than a uniform federal plan?

3. Will my plan resolve, rather than exacerbate, the disconnection between law enforcement agencies?

4. Am I strong enough, and do I have the integrity to put aside my ego and need for control for the greater good?

Our choice is a simple one. Do we want to have an effective fight against terrorism, or are we more interested in grabbing a piece of the federal funding?

Cost Factor

The Federal Liaison Training Program can be accomplished with the expenditure of $5,000,000 or less. Dozens of independent local and state programs may cost hundreds of millions of dollars.

Time Factor

The Federal Liaison Training Program can deliver training to virtually every police officer and can certainly provide the liaison resource within six months. The review of grant applications and distribution of funds for the initiation of the multiple local and state programs will not be accomplished within six months. It is doubtful that we can expect the terrorists within our country to wait until we are prepared.

Quality Factor

There can be no question that a federal program developed through our national experts would be far superior to any local or state program. The federal model will provide lecture content, handout materials, and training aids from our most expert federal authorities. The end product will be consistent information and uniform national protocols.

The local/state model will employ various local, state, private, and federal experts with varying levels of expertise and information. This fragmented training will result in multiple protocols and little unified effort.

Disconnection Factor

The disconnection factor is the most important component of a federal liaison program. The primary goal is to create a level of trust between our law enforcement agencies which can be fostered by federal officials knowing that the liaisons receiving and sending information have been trained by them. Multiple local and state programs will not accomplish this goal and may, in fact, exacerbate the disconnection.

The choice is obvious, and the ability to immediately accomplish this training goal is easily within our reach.

Elliot Spector was employed as a police officer by the City of Hartford from 1971 to 1980. He presently is in private practice in a firm he founded which specializes in defending police officers and bringing actions for officers and their family members who are injured or harmed due to the negligence or misconduct of others.

He provides legal advisory services to a number of local police departments. He presently serves in a legal advisory capacity on projects for the National Institute of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Agency.

Since 1991, he has provided the liability training for attorneys across the country who specialize in representing police officers at the annual IACP Convention. He has a regular legal update series which appears on the Law Enforcement Training Network and is the President of the Connecticut Criminal Law Foundation, Inc.'s Center for Police and Security Training, a nonprofit teaching organization for law enforcement.

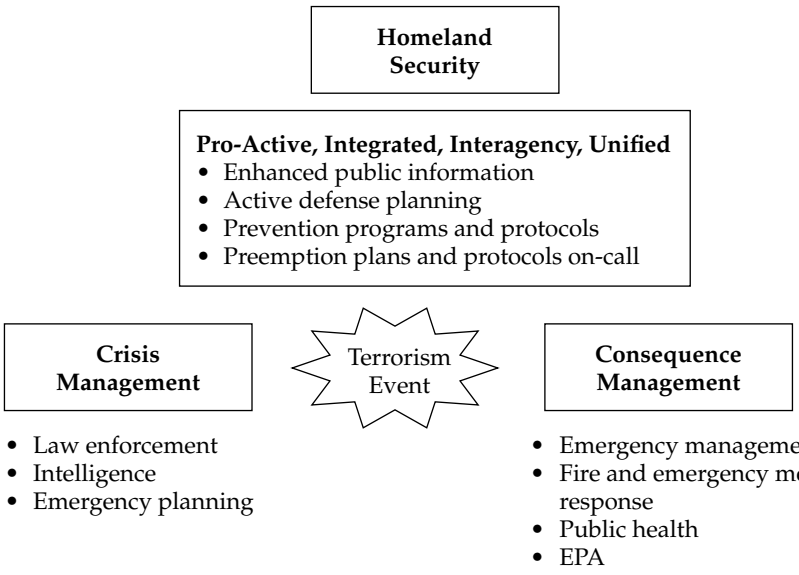
He is past-chair of the Legal Officers' Section of the International Association of Chiefs of Police and served on its Executive Board. He has also served for many years on the Legislative Committees of the IACP and CPCA.

"Homeland Security": Active Measures to Prevent and Preempt Terrorism

Richard L. Jaehne, Director, Illinois Fire Service Institute

For the past several years, the U.S. has been pursuing a strategy of "Crisis Management" (law enforcement and intelligence conducted before a terrorist event) and "consequence management" response and recovery.

In order to protect the United States against current terrorism threats, the U.S. needs to create a "bridge" of active defense measures between these two concepts. Our goal should be to provide *active* planning, prevention, and preemption measures, plans and protocols to lessen the effect of or stop terrorist attacks. Over the years, we have called this "Civil Defense," "Domestic Preparedness," and now "Homeland Defense." The challenge is to do it in the interagency stewpot of domestic law enforcement, public safety, and elected officials, in a unified way at the local and state leadership level.



Our central challenge in the months and years ahead is to move to active security. Specific initiatives should include the following:

- Develop discrete Homeland Security THREATCON levels and measures that parallel the military THREATCONs
- Creation of an integrated set of national-state and key metropolitan city intelligence and operations interagency "fusion centers"
- Creation of a small, inter-agency "critical targets" analysis and planning group to conduct contingency analysis planning
- Clear articulation of the critical decisionmakers and decisionmaking process to be used in the event of an imminent threat warning/terrorist event

Recommended Illinois Actions

On May 16, 2000, Governor George Ryan signed Executive Order Number 10 (2000) formally creating the Illinois Terrorism Task Force (ITTF). Under the leadership of the Deputy Governor for Public Safety and Director for Homeland Security Matt Bettenhausen and Illinois Emergency Management Agency (IEMA) Director Michael Chamness, the Task Force will continue to provide the interagency forum to direct state efforts toward planning, preparation, and response to terrorism in Illinois. Today, through interagency cooperation of the Terrorism Task Force members Illinois has . . .

- A fully operational State Interagency Response Team with two more in training to be operational by the first of the year.
- Terrorism training curriculum and instructors in place to reach every first responder statewide.
- A state inter-agency command and control system to plan and direct support for counter–terrorist response, to include statewide fire service mutual aid.
- 27 HAZMAT level A technical teams, more than special rescue teams, bomb squads, dog teams, and other specialized teams equipped from local sources to assist statewide. Many of these teams have attended national training.

In order to more effectively protect Illinois, each local jurisdiction and public safety entity must be part of the planning, preparation, and preemption efforts described below. In Illinois, our goal should be . . .

To establish a *proactive, integrated, layered, active* defense shield against terrorist attacks on critical Illinois infrastructure.

Historical Framework. Reviewing how America and Illinois responded to the call for active civil defense in World War II and in 1961-1962, three components were critical. Implementation of Homeland Security post September 11, 2001 should build on these three critical historic actions:

1. Creation of universally understood, integrated, yet flexible early warning systems from local to state and national levels

2. Implementation of a broad-based public information campaign to inform each citizen (to include school children) about the terrorist threat and what each can do to help protect against the threat

3. Creation of a series of small interagency teams that developed and implemented specific programs to counter the threat and respond to catastrophic events

GAO Analysis. Post-September 11, 2001, the General Accounting Office identifies three requirements, based on a Department of Defense approach (specific reports available at <www.gao.gov>):

1. *Assess threats* posed by individuals and groups, and implement actions to "eliminate or reduce the threats."

2. *Identify vulnerabilities and weaknesses* in infrastructure, operations, planning, and exercises; and then identify steps to mitigate them.

3. *Assure ability to respond and mitigate attack consequences*.

In developing Illinois' state structure/response, we should recognize that homeland defense against terrorism is a national problem that will be played out at the local level. Proactive leadership is a critical component at every level.

Task #1 – Early warning system

- Re-tool and expand the existing "early warning system" to incorporate terrorist THREATCON measures based upon the military THREATCON system but with discrete measures appropriate for local communities and critical Illinois infrastructure. The Joint military publication 3-07.2 *Joint Tactics, Techniques and Procedures for Antiterrorism* is available at <www.adtdl.army.mil/cgi-bin/atdl.dll/jt/3-07.2/default.htm>. This document identifies five THREATCON levels:

    1. THREATCON NORMAL – General threat of terrorist activity exists but warrants only a routine security posture.

    2. THREATCON ALPHA – General threat of terrorist activity is possible, and increased security posture is warranted.

    3. THREATCON BRAVO - General threat of terrorist activity is increased, and specific threats are predicted.

4. THREATCON CHARLIE – A terrorism incident has occurred, or intelligence is received that an attack is imminent.

5. THREATCON DELTA – A terrorist attack has occurred, or intelligence indicates that an attack against a specific location is expected—highest security level.

Each of these THREATCONs has a series of discrete security "measures" that should be considered in the development of local protocols.

- Creation of Terrorist Early Warning (TEW) groups in Chicago for the Chicago metropolitan area and in Springfield for national-state interface and for the remainder of the state. The model for these groups is the Los Angeles County effort led by the Sheriff's office. A case study of the Los Angeles group is contained in the Gilmore Report entitled the "Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction" available at <www.rand.org/nsrd/terrpanel/terror2.pdf>.

  - Groups must have interagency representation including local, state, and federal representation and should be led by law enforcement.

  - Missions

    - Create an indications and warning intelligence collection, assessment, production, and dissemination process.

    - Conduct critical target and net assessment.

    - Conduct joint operational planning and mission direction.

  - Tasks

    - Build critical infrastructure target list (commercial, financial, informational, and political, etc.).

    - Conduct functional infrastructure analysis by both target and functional area (cyber, bio, chemical, biological, nuclear, massive conventional explosion, etc.).

    - Build critical infrastructure target folders with defense, preemption, and response plans and protocols.

  - Groups should employ IPB (Intelligence Preparation of the Battlefield) to create a tailored set of analytical models for Illinois. IPB is a systematic process to analyze the threat and environment that seeks to do the following:

    - *Template Threat* - Determine the threat's likely course(s) of action (COA).

    - *Define Environmental Factors* - Define the operating environment in which the threat will act.

    - *Plan Response* - Define actions that should be taken to prevent, preempt, and/or respond to the threat's likely COA.

- More information on IPB is available at <155.217.58.58/cgi-bin/atdl.dll/query/download/FM+34-130>.

Task #2 - Public information campaign

- Designate and empower an interagency group to design and implement the campaign. Governor Ryan began a series of workshops on October 29, 2001 around the state to kickoff this effort. In additional, the State Terrorism Task Force is forming a subcommittee to address this as an ongoing issue.
  - Include all Illinois citizens and special interest activities.
  - Conduct a baseline public survey on citizen perceptions of security, actions they have/will take, expectations for security actions, and follow-up with re-surveys to judge and allow response to changes in citizen perceptions.
  - Market using multimedia, paid and public service announcements, tailored products targeted to reach specific groups and themes.
  - Local jurisdictions must play an active role in this effort.
- Conduct Leadership workshops and statewide summits on homeland defense to achieve leadership "buy-in." The overall goal of the workshop is to improve actual and perceived homeland defense security against terrorism in Illinois.
  - Provide specific critical homeland defense information.
  - Identify and take actions to improve homeland defense and public sense of security.
  - Bring together interested parties who can create and implement an action agenda to improve real and perceived security for homeland defense.

Task #3 - Interagency teams

Traditional civil defense and natural disaster response had four phases: (1) Awareness, (2) Alert, (3) Warning, (4) Response. Homeland Defense must add "Preemption" between "Warning" and "Response." The Los Angeles County TEW system is instructive on what groups should be formed. Illinois should have/form:

- State Terrorism Task Force – Continue and augment the ability of the Terrorism Task Force to develop and implement homeland defense policy statewide.
  - Continue to build a statewide program for equipping, training, and supporting first responders.
  - Inter-agency policy "think-tank"
  - State EOC and EAP participants

- Terrorism Early Warning (TEW) groups – Create two full-time TEW groups dedicated to intelligence (collection, analysis production, and dissemination) and operational planning.

- Local Planning – Build interagency homeland defense planning and preparation committees in local communities by enhancing regional and local emergency management plans and processes.

- Conduct training and exercises to enhance homeland defense command and control, planning, and response capabilities.

  - Focus on unified command processes.

  - Train and exercise on homeland defense scenarios.

  - Include technical experts to help improve our processes.

For more information, contact the Illinois Emergency Management Agency, any member of the Terrorism Task Force or the author at <jaehne@uiuc.edu>.

Richard L. Jaehne was appointed as the director of the Illinois Fire Service Institute on August 21, 1997. The Institute is the statutory State Fire Academy, and the Director is the Illinois State Director of fire service training. The Institute has 350 full- and part-time faculty and staff who deliver over 300,000 student hours of training to over 27,000 firefighters annually.

He is the codeveloper of the seminar entitled "Where the Battle Begins," which relates leadership in high-risk situations between the military and fire service. He is a member of the Illinois State Fire Commission, of Illinois Governor Ryan's Blue Ribbon Fire Service Committee and State Terrorism Task Force and cochair of the State Terrorism Task Force Training subcommittee. He is the immediate past Vice President of the North American Fire Training Directors (an international association of the state and Canadian directors of fire training) and a member of the National Fire Service Leadership Summit. He is on the editorial board of the *International Journal of Emergency Mental Health*. He created and implemented a memorandum of Agreement with the Russian Interior Ministry for cooperative fire science education, training, research, and exchange. He was awarded a faculty appointment in the Russia and East Asia Institute in 1999.

He retired from the U.S. Marine Corps as a colonel. During that time, his association with crisis management included assignments as the Director for Marine Corps Operations worldwide where he oversaw operations of the Marine Corps Crisis Action Center, Marine disaster relief assistance with FEMA, and mutual support efforts with the Federal Bureau of Investigation and other federal agencies. While commandant of the NATO School, he also established a mutual support program in civil-emergency operations training, sending NATO training teams to Russia and hosting Russian instructors at the NATO School.

Weapons of Mass Destruction and Terrorism: Illinois' Preparatory Response

Michael P. Moos, Program Manager, Illinois Law Enforcement Training and Standards Board
Richard Jaehne, Director, Illinois Fire Service Institute

September 11, 2001, a day that will live in infamy for public safety. Many states across the nation are trying to develop and implement plans, training and abilities so they will be able to address terrorism if it comes to their front door. Illinois though has been at the forefront, addressing Weapons of Mass Destruction (WMD) and terrorism issues for the last two years. This paper provides an overview of Illinois preparatory response.

Terrorism's history in this country is recognized only recently with the advent of large-scale events that have been ingrained into our minds. The mixture of domestic (Unabomber, Oklahoma City) and international (Pentagon and World Trade Center) terrorism makes civil defense era plans not as trivial as they had been perceived. Every state in this great nation of ours must face how to address WMD/terrorism with utmost care and expediency.

The State of Illinois, for the last two years, has endeavored on an expedited basis to address how to prevent and react to WMD/terrorism acts. We have been able to address and assist in many large scale events, such as the World Soccer matches, Democratic National Convention, or the Pope visiting; but to be ready as a state, we needed a master plan. On May 16, 2000, that master plan became a reality with the advent of Governor George H. Ryan signing Executive Order #10 into effect. This Executive Order brought the framework of state activity into action by officially forming the Illinois Terrorism Task Force (ITTF) whose goal it is to protect the lives and property of citizens and visitors to our state.

While the governor made it official on May 16, in reality, the ITTF had been meeting on a monthly basis since October 1999. The task force is chaired by the director of the Illinois Emergency Management Agency (IEMA), with the vice-chair represented by the Illinois State Police. The task force itself is represented by 33 local, state, federal, and private entities (see Attachment A for the ITTF roster) whose role it is to assist in the planning, training, implementation of programs, protocols, and response to a WMD/terrorism incident.

The task force is also divided into four subcommittees:

1. **Bio-Terrorism and Health Committee**, Chaired by the Illinois Department of Public Health (IDPH)

2. **Crises Response Committee**, Co-chairs are the Illinois State Police and the Illinois Environmental Protection Agency (IEPA)

3. **Training Committee**, Co-chairs are the Illinois Law Enforcement Training and Standards Board (ILETSB) and the Illinois Fire Service Institute (IFSI)

4. **Communications Committee**, Chaired by the City of Chicago Emergency Services and Disaster Agency (Chicago ESDA)

On December 31, 2000, the ITTF submitted to Governor Ryan the task force's report of activities and recommendations to assist in laying the foundation for further actions. Utmost of concern to the task force, was local and state abilities to respond to WMD/terrorism events. With that in mind, the following initiatives were identified and action taken.

Response from the State

If a community or region is affected by a WMD/terrorism event, it is expected that local resources would be stretched to the limit and the state might need to provide assistance. The State Interagency Response Team (SIRT) was formed to respond to a WMD incident anywhere in the state within 60 to 90 minutes of notification and to provide all avenues of support to the local incident commander and the appropriate federal agencies responsible for the mitigation and investigation of such an incident. Three teams have been formed located in the Chicago area, Springfield, and the St. Clair County area. Each SIRT is comprised of State Police Tactical Response Team (TRT) members plus representatives of the Secretary of State Bomb Unit, IEMA, IEPA, Nuclear Safety (IDNS), IDPH, Office of the State Fire Marshal (OSFM), and local liaisons. The SIRT teams are trained not only in their specialty area but also in over 152 hours of hazmat and incident command training:

- Hazardous Materials Awareness (8 hours)
- Hazardous Materials Operations (40 hours)
- Hazardous Materials Technician A (40 hours)
- Hazardous Materials Technician B (40 hours)
- Emergency Response to Terrorism – Basic Concepts (16 hours)
- Unified Command for Incident Command (8 hours)
- Specialized training as identified (i.e., bomb schools, etc.)

According to the Chairman of the Illinois Terrorism Task Force, Michael Chamness, the SIRT has many functions to offer, utmost is that they are to "support local government responders as a resource . . . not to take over." The SIRT can provide many functions such as scene stabilization, establishment of an inner perimeter, neutralization of human threat(s), and provision of initial detection of hazmats and chemical and/or biological agents. The SIRT can render aid to victims and decontaminate victims, emergency responders, and all items moving from "hot" to "cold" zones. The SIRT will preserve the crime scene and provide communications to incident command and the State Emergency Operations Center (SEOC). The SIRT will be the advance preparation team setting the stage for the arrival of the Illinois National Guard Civil Support Team, including providing for a decontamination corridor. Finally, the SIRT will act as a liaison to the FBI. It should be noted that the SIRT will establish an incident command system until local incident command is established.

Response from the Local Level

The World Trade Center attacks made it evident that any event would immediately tax local and state resources. The fire service in Chicago and collar county areas utilize the Mutual Aid Box Alarm System (MABAS) as a means to resolve lack of resources and a means to ensure that all communities have immediate protection when all resources are obligated to a large fire-service-related emergency. MABAS basically set the template for the rest of the state. Under the leadership of the Illinois Emergency Management Agency and the Executive Board of MABAS, an agreement has been made to expand MABAS statewide as a state asset. Now, we find that if an event occurs, resources from anywhere in the state could be available.

Is such a system viable for law enforcement? This has yet to be resolved, but it seems appropriate that we embrace this concept so that resources from throughout the state are available. At the time of the paper, the IACP is investigating this concept.

Equipping First Responders and State Responders

It is the goal of the state to ensure that it has the capabilities to respond to an event with the resources to do so. The SIRT needed to be equipped with Self Contained Breathing Apparatus (SCBA) that did not inhibit their law enforcement functions. Level A and B suits, decontamination equipment, detection monitors, and hazmat mitigation equipment were required to be purchased to ensure the state could assist local government. The state also identified local Hazardous Material Technician A response units that needed specialized detection equipment. Finally, the State identified Technician B units that needed to be trained and equipped to perform at the Tech A level. It is the intent to have these specialized units available as regional response units for the state.

Coordination of Funds

The State of Illinois and some key counties in the state have qualified for federal funds to assist in their WMD/terrorism goals. The task force is working to ensure that no duplication of efforts for valuable monetary resources are available to the state and that we are not competing with one another. It is imperative that funds be received not only by cities within the state, but those areas in need that may not qualify as well due to their rural status.

Training Initiatives

The training subcommittee devised an ambitious but reasonable plan. The training goal is to improve local, regional, and state interagency and unified command response to terrorist incidents involving conventional, chemical, biological, or nuclear weapons. The subcommittee identified seven training objectives to guide direction.

Objective 1: To provide SIRT training

At the time of this paper, the Central Team has been activated. The Northern and Southern Teams will be activated by mid-December (CY01). The training

subcommittee recommended that all SIRT team members go through the training together from Operations through Technician A levels to develop team cohesion and to ensure that the team understood what was required from each other in order to operate in the "hot" zone.

Objective 2: To fulfill the need for WMD/terrorism training for first responders statewide

There have been many courses available by the "Training Triad" (ILETSB, IFSI, and IEMA) for first responders of which many are provided through grants. The following are currently available:

- Hazmat Awareness
- Hazmat Awareness Refresher (classroom or web-based training available)
- Hazmat Operations
- Hazmat Technician B
- Hazmat Technician A
- Emergency Response to Terrorism – Basic Concepts

Common Glossary of Terms

As with any multi-agency, multi-level organization(s), we become inundated with terms that may not be familiar or are interpreted by law enforcement one way and the fire service another. The training subcommittee developed a "Common Glossary of Terms" that summarizes many of the acronyms utilized by the military and public safety. It is our hope that such a document might alleviate any confusion before we are called into action.

Training Facilities

The state would utilize existing training institutions to assist us in meeting our goals. ILETSB would utilize its 16 inservice training regions of Mobile Team Units (MTUs) and six basic training academies. The Illinois Emergency Management Agency would utilize their Regional Coordinators, and the Fire Service Institute would utilize its academy and Regional Training Centers.

Training is focused on four groups. First and utmost are the SIRT teams; next are the first responders in the state and thirdly all local and state governmental employees. Finally, we recognize that training of public officials and the public is necessary, especially with the advent of a "swell" of concern from the public.

In order to provide such training, the triad of training organizations reviewed and dovetailed the Department of Justice's (DOJ) "Emergency Response to Terrorism – Basic Concepts" (ERT-BC) course to the needs of Illinois. The course was finalized in the summer of 2001, and instructor train-the-trainer courses were held to bring present law enforcement, fire service, and emergency management hazmat instructors up to speed with this curriculum.

The ERT-BC course in Illinois is broken down into two sections: a basic eight-hour, five-module course for all public safety entities, and (2) an additional four-hour session available for detection and treatment training.

The modules are broken down as follows:

Module 1: Understanding and Recognizing Terrorism will help the responder recognize suspicious circumstances in advance.

Module 2: Implementing Self-Protective Measures assists students in utilizing time, distance, and shielding to protect themselves from dangerous exposures.

Module 3: Scene Control defines isolation, evacuation, and control issues unique to terrorism incidents.

Module 4: Tactical Considerations covers specific defensive measures utilized in each major category, "B-NICE" (Biological, Nuclear, Incendiary, Chemical and Explosive), incidents.

Module 5: Incident Command Overview gives a broad picture of . . .

- Local, state, and federal resources.
- Making appropriate notification.
- Specialized crime scene consideration.
- Operating in a multi-jurisdictional command system under the Federal Response Plan (FRP).

The course ends with a final activity and final exam. The additional four-hour training module (for those agencies that identify themselves having such a job task) provides training in the following:

- Detection equipment and measures.
- Treatment protocols and procedures.

Objective 3: To fulfill the need for Incident Command Training for first responders; to provide training for Emergency Operations Center (EOC) operations

Incident command has been labeled with a multitude of names as it has evolved or been adopted by different services throughout the country. Incident Command System (ICS), Critical Incident Response (CIR), and the Incident Management System (IMS) are just a few examples of such names. Each provides training in a field resource system that is utilized to keep a small to large event efficient and organized. The fire service and emergency management has adopted such a system in their field operations for many years. Federal rules (CFR 29 part 1910.120) mandate the use of such a system when first responders deal with hazardous materials events. It is imperative that law enforcement learns that ICS is a tool that can be utilized for everything from a traffic accident, to a hostage situation, to a terrorist act. The Illinois State Police embraced this concept and has trained every trooper and command staff in ICS. It should be noted that the Illinois State Police Academy training program has become popular and is offered through the ILETSB inservice training regions. Based on the "Bomac" program, this 24-hour course teaches the officer basic ICS principles and how to apply them in the field. Key to the teaching is the use of a large-scale model city that provides students opportunities to "play out" scenarios ranging from traffic accidents, to hostage scenes, to hazmat incidents, to a terrorist event.

Unified Command for ICS is a new eight-hour course designed to provide multi-agency command level officers and mayors, managers, and/or county board chairmen the orientation and training to operate under the Unified Command System. In addition, IEMA has available an Emergency Management Institute (EMI) Emergency Management Course for EOC training.

Objective 4: To provide specialized training to prioritized teams

The state has identified five hazmat teams that need to be upgraded from Technician B level to Technician A level. This will also require a review of equipment, training, team sustainment costs, and support of the local community to bear such responsibilities.

An overall review of fire service specialized rescue teams is in the process of being conducted by MABAS to ensure what is available as statewide assets. In the aftermath of the World Trade Center attacks, there has been renewed discussion of establishment of a national Urban Search and Rescue (USAR) team in the Chicago area for Illinois.

SIRT, SIRT instructors, Hazmat Technician A, Specialized Rescue teams, TRT, Bomb Squad, K-9, Clandestine Drug Lab, and other specialized entities and their instructors, need to stay abreast of current techniques and equipment that permits efficient operations in the field. The task force will identify such training and prioritize entities to utilize such training, including national level training.

Finally, such training and organization of teams needs to ensure that any area of the state will be adequately covered by special capability teams.

Objective 5: To create a program for public awareness of terrorism

The significance of this objective has grown dramatically in the wake of September 11. The training subcommittee has recommended that a new committee be formed to focus on the goals of this objective.

Objective 6: To achieve "Buy-In" by key elected and public safety decision makers at the local, regional, and state level for Homeland Defense Training

The training subcommittee feels that a "Top Down" approach is necessary to ensure support for local first responders. This was further emphasized and started when Governor George H. Ryan held a meeting on October 15, 2001, for cabinet level leaders and top law enforcement, fire service, and emergency management officials on the state's position on terrorism. This was followed up by regional homeland defense briefings, which were held throughout the state, providing insight to the state's ability to address WMD/terrorism emergencies. The training subcommittee intends to follow up these briefings with planning workshops for local and regional government officials and first responders. The goal will be to bring together those who can create and implement an action agenda to improve real and perceived security for homeland defense. We intend to culminate the workshops with a statewide summit cosponsored by the University of Illinois as a Partnership Illinois program.

Objective 7: To provide weapons of mass destruction/homeland defense training to public health and medical preparedness and response staff

The Illinois Department of Public Health has set the groundwork for EMS First Responders, health departments, and hospitals in addressing WMD/terrorism events. Their roles are multifaceted from responding to emergencies in the field, to analyzing influx of signs and symptoms in clinics, to providing medical attention to those affected by an event. There is an impetus for additional training that will be addressed by the task force.

Training Summary

While much has been accomplished, it has become evident that we have much more to do in order to meet our goals. In summary, the training subcommittee has developed four pillars that support our project goals through 2002.

Generate public awareness and support for terrorism and homeland defense training.	**Achieve awareness and buy-in by key decisionmakers for homeland defense.**	**Establish fully operational statewide special response teams.** SIRT, Hazmat A Teams, Special Rescue Teams	**Establish and expand statewide mutual aid system public safety networks.** Fire, EMS, Law Enforcement

Summary

Today, Illinois has an interagency anti-terrorism training strategy with seven clear objectives, current curriculum, a trained network of more than 200 instructors, established places throughout Illinois to train, with some of the training available on the internet. We need only to connect to the first responders who need to be trained. Making first responders available for training must be a local priority. Together, we can reach first responders in every Illinois community in a matter of months and move the percentage trained on Basic Concepts of Terrorism and Terrorism Awareness to 50% or more within six months. This will take a focused partnership effort at the local and state level.

It is our responsibility to do so . . . so that we can meet the public's expectations of public safety to mitigate the loss of life and property in case of a WMD/terrorism event.

Michael Moos earned his BS in education in 1975 and his MS in occupational safety in 1976 from Illinois State University and has been active in the fire, EMS, emergency management, and law enforcement professions for 25 years. He represents the Illinois Law Enforcement Training and Standards Board on the Illinois Association of Chiefs of Police Terrorism Committee and the Illinois Terrorism Task Force and is co-chair of the task force's training subcommittee. Prior to his service with the board, Moos was program director

of the State of Illinois' 911 Program and just recently retired as assistant chief of the Sherman Fire Protection District.

Richard Jaehne is the director of the Illinois Fire Service Institute which is the statutory state fire academy. He is codeveloper of the seminar entitled "Where the Battle Begins," which relates leadership in high-risk situations between the military and fire service. He is a member of the Illinois State Fire Commission, of Illinois Governor Ryan's Blue Ribbon Fire Service Committee and State Terrorism Task Force, and co-chair of the State Terrorism Task Force Training Subcommittee. He is the immediate past vice president of the North American Fire Training Directors (an international association of the state and Canadian directors of fire training) and a member of the National Fire Service Leadership Summit. He is on the editorial board of the *International Journal of Emergency Mental Health*. His formal studies include BS in business and financial management from the University of Utah and an MS in systems management from the University of Southern California.

Attachment A

Illinois Terrorism Task Force Member Agencies

- Illinois Emergency Management Agency (Chair)
- Illinois State Police (Vice-Chair)
- Governor's Office
- American Red Cross (ARC)
- Associated Fire Fighters of Illinois (AFFI)
- City of Chicago
- City of Chicago ESDA
- Cook County ESDA
- DuPage County ESDA
- FBI (North and South)
- Federal Emergency Management Agency (FEMA)
- Kane County ESDA
- Lake County ESDA
- North Aurora ESDA
- Illinois Association of the Chiefs of Police (IACP)
- Illinois Association of Public Health Administrators
- Illinois Attorney General
- Illinois College of Emergency Physicians
- Illinois Department of Agriculture
- Illinois Department of Military Affairs
- Illinois Department of Nuclear Safety (IDNS)
- Illinois Department of Public Health (IDPH)
- Illinois Department of Transportation (IDOT)
- Illinois Emergency Services Management Association (IESMA)
- Illinois Environmental Protection Agency (IEPA)
- Illinois Fire Chiefs' Association (IFCA)
- Illinois Fire Service Institute (IFSI)
- Illinois Hospital and Health Systems Association
- Illinois Law Enforcement Training and Standards Board (ILETSB)
- Illinois Office of the State Fire Marshal (OSFM)
- Illinois Secretary of State Police (SOS)
- Illinois Sheriffs' Association (ISA)
- Mutual Aid Box Alarm System (MABAS)
- U.S. Attorney's Office

Common Sense Solutions for Homeland Security

Michael R. McKinney

September 11, 2001 served as a wake-up call to law enforcement and public safety agencies throughout the country to respond to the long predicted assault by terrorism on the continental United States. The terrorists had hoped to cause mass hysteria within our governmental and financial communities, leading to a collapse of our way of life. Obviously, they misjudged the will power of our populace. This wake-up call has resulted in a movement to research new ways to protect our homeland and be prepared for the poisons that 21st century terrorists hope to spread. The mass purchase of gas masks, the canceling of corporate events and near collapse of the aviation industry has instilled not only an increased level of concern but in some cases unwarranted fears and nightmares of events that may yet come. While international terrorists and commercial burglars have very different motives, they also have similarities that can be attacked in a similar manner. Both are criminals and because of this association, they do not want to be caught; they work in the shadows away for scrutiny, and they seek out weaknesses in security to accomplish their goals. Perhaps we should revisit our security plans that emphasize crime prevention techniques and applications by citizen and police partnerships as a front line defense in the war on terrorism and improving homeland security. The application of these time proven techniques of crime prevention can yield increased citizen awareness and preparedness without feeding hysteria and fear.

Security Barriers – The Three Levels of Defense

Traditional crime risk management identifies three basic levels of defense in the anticipation, recognition, and appraisal of crime risks and the initiation of action to remove or reduce crime risk. Many applications of the subcomponents of these three levels of defense can directly serve as a deterrent against terrorist incidents as well as less sophisticated criminal acts.

Level I – Perimeter Barriers

Perimeter barriers define the outside or perimeter of a site and represent a physical and psychological deterrent. These barriers do not provide complete protection and can only be expected to delay intrusion. Perimeter barriers require regular maintenance and inspection and serve to channel vehicles and people in emergencies. Some traditional types of perimeter barriers that can aid in preventing a terrorist incident include fencing, certain types of landscaping and shrubs, security towers, motion detection systems, and lighting. Modern applications of the perimeter barrier include concrete highway barriers to divert and deter any type of vehicle-related explosive or incendiary device and decorative planters anchored in concrete to blockade public entrances.

The use of multiple types of perimeter barriers in tandem can greatly multiply the amount of perimeter protection. One modern application is the use of portable

lighting on those areas of fenceline that have limited traditional lighting. This will increase the visual deterrence of the fence and aid in observation and detection by security personnel. The portable lighting could be used in tandem with concrete barriers to not only illuminate the barriers as a deterrent, but also serve as a concealment to security checkpoints. Other types of modern perimeter barriers with terrorism applications could include increased visual patrols, enforced policies on access to restricted areas, and the use of ionization devices and explosive detection canines.

Level II – Building Exteriors

The survey and consideration of building exteriors must include not only all sides of the structure, but also the top and bottom of the structure. The traditional applications have always concentrated on the hardening of the target by use of solid doors with heavy-duty hardware and protected locks and hinges as well as permanently securing ground level windows or the use of window mesh and inside pins. While these areas need to be inspected, attention should also be given to the inspection and securing of sewer and storm drains and manhole covers. Roof areas should be inspected for the use of strengthened and reinforced building materials enhanced by a motion detection system. Ventilation systems are traditionally difficult to secure but should be a priority with the threat of use of biological and chemical agents by terrorists. Utility poles, fire escapes, trash dumpsters, and other types of structures that allow physical access to the roof areas or upper level windows should be relocated.

Modern applications for hardening building exteriors include facial imaging systems, retinal identification, and voice recognition systems. Again, the use of multiple systems of protecting building exteriors can greatly multiply their effectiveness. These types of protective applications should not be strictly limited to buildings; they should also be applied to vehicles in mass transportation. One example is the strengthening of airplane cockpit doors. Security of these doors has been accomplished by titanium reinforced hinges and locking mechanisms with similar titanium covers and armored solid doors. This is a modern application of improving on hollow wood doors and hinges as well as traditional cylinder type locks on older building exteriors.

Type III – Interior Controls

Interior controls relate directly to the nature of the work involved at the site. Traditional examples of interior controls include strict key and tool control, restricted access identification, increased security of areas that store data, checks or drafts including invoice orders, and travel documents. The use of flood lighting can serve as a visible deterrent. As with certain exterior controls, the enforcement of policies on the entry of restricted area and increasing the number of employees needed to open a business can yield a more security-minded workforce. Interior controls could include policy on suspicious mail and packages, procedures for the handling of such packages, or the receipt of bomb threats and special consideration to employee safety in high rise buildings.

Executive Security

None of us are immune to the possibility of becoming a victim of a terrorist act or other violent crime. Business executives are potential targets for acts of terrorism. Traditional security plans should be "dusted off" and include contingency plans for terrorism. Executive security can be divided into four basic categories:

1. Office Security
2. Home Security
3. Lock Security
4. Travel and Vehicle Security

1. Office Security

The basis of an effective office security program is a professional independent security survey. This survey will address physical concerns as well as procedural guidelines, security resources, target potential, and target evaluation.

Physical security should be developed around security offices, electronic countermeasures, and common sense. Some effective guidelines include the following:

- Removal of all potted plants and ornamental objects from public areas
- Close surveillance and identification of visitors
- Upgrade and enforcement of access control systems
- Duress alarms
- Bomb threat and search plans
- Strict screening and inspection of mail and packages
- Trash emptied frequently
- Removal of names from offices and parking areas

2. Home Security

Home protection is the most difficult area in the overall executive security program to deal with. Age differences, marital troubles, and preoccupation with social and business activities are all problems which tend to change the family security profile. Steps to increase home security include not only the application of traditional crime prevention target hardening as explored earlier in the three levels of defense, but also . . .

- Training the family to be a stronger psychological unit under stress.
- Conducting a comprehensive security survey that not only addresses security needs, but also emergency plans and safety equipment
- Establishing a home security program that is based on proven security principles and hardware and reinforced with dedicated family participation from all members

3. Lock Security

The security of the residence, office, and vehicles will rely heavily upon physical locking devices. As important as the locking device is, the security afforded is only

as good as the construction of the door and frame. The most significant hazard when considering door and lock security is the door that fits loosely to the frame, thereby allowing it to be pried or forced open.

4. Travel and Vehicle Security

The ease of access makes the vehicle the ideal place to apply scare tactics and warnings and gain initial control of the executive or family member. Actions and policies can be developed to minimize the executive's risk and complicate the terrorist's plan. Basic travel security policy is divided into three components:

1. Normal travel procedures
2. Vehicle protection
3. Attack simulation procedures

All three areas include defensive driving and vehicle attack training, avoiding routines, security of the vehicle indoors, back-up communications, and safety equipment including "run flat" tires and armoring. Travel plans should be restricted to a "need to know" basis. Always be alert to possible surveillance, and be aware of minor incidents that can block traffic.

Business Controls for Terrorism Awareness and Crime Prevention

One of the most constant problems facing every businessman is ensuring that employees are both productive and honest. Many of the crime prevention tools used to accomplish objectives can be successfully implemented to help prevent possible acts of terrorism and strengthen defenses against such "ordinary crimes" as theft, burglary, and robbery. Management must strive to work closely with employees to ensure that increased security measures do not interfere with production or viewed as a counter-productive expense. The same opportunities that allow for the theft of merchandise can also provide opportunities for the terrorist to obtain materials for the production of potential weapons of mass destruction. Some general steps that can be taken to tighten controls of property and merchandise, thus deterring terrorists and common criminals include the following:

1. Receiving Merchandise

- Limiting the hours of receiving to specific times
- Posting the schedule on the dock door
- Assigning three different employees for duties concerning receiving, store keeping, and delivery handling
- Receiving within a fenced area
- Eliminating blind spots so receiving clerks can observe the entire area
- No employee or unauthorized vehicles within 50 feet of the receiving door
- No employee leaving the building through the receiving door
- Deliveries not remaining on loading dock
- Doors or gates locked when not in use; buzzer or intercom alerting staff of a waiting delivery
- Inspection of deliveries and not simply approving them from packing slip
- Weight of the product
- Seals on rail can and trailers

- Delivery drivers not allowed past the immediate dock
- Factory sealed cartons
- Inventory delivery vehicles at loading
- Vehicles always locked
- Cargo loss
  - Parking of trailers back to back
  - Marking on all sides including top
  - Top locks on doors
  - Lighting
  - Nonstop hauls or convoys, security escorts

2. Warehouse and Storage
- View the warehouse like a banker views the vault.
- Restricted access to warehouse and storage areas
- Color coded badges, electronic ID, and coded locks
- Mgh value good area - Constantly attended when not locked
- Video surveillance

3. Employee Controls
- The more time spent in pre-employment screening, the better the employees selected.
- Background and criminal history checks
- Promotion of employee employment stability
- Control of employee entry, exits, and parking

Summary

Terrorists win by causing fear and disruption in our way of life, but we cannot give in to their demands or threats. The combination of tried and true crime prevention techniques and applications with modern technology is a winning combination to thwart potential terrorist actions and prevent violent crime. Practicing a security philosophy of prevention, preparedness, and planning will allow each of us to defend our homeland in a common sense and practical manner while avoiding the hysteria and disruption sought by the terrorists.

Michael R. McKinney is a 26-year criminal justice professional who recently retired after a much decorated career with the Sangamon County Sheriff's Department and the Illinois Department of Corrections. McKinney's career includes an all-encompassing combination of law enforcement experience in the areas of administration, investigation, training, emergency management, and operations. McKinney continues his career, serving as a municipal police officer with the Leland Grove, Illinois Police Department. He is the president of McKinney and Associates, a law enforcement training and consulting group in Springfield, Illinois.

McKinney has served in special operations assignments throughout his career, including SWAT team member, terrorism task force investigator, statewide special operations response team member, EMT-paramedic, executive protection special agent, statewide canine administrator, and criminal street gang crime specialist. He is a seasoned public speaker and

law enforcement trainer, having developed, organized, and instructed over 150 presentations on combating violent criminal gangs. McKinney is also the recipient of the Governor's Special Award of Valor, the Illinois Department of Corrections Special Achievement Award, Employee of the Month, and the U.S. Department of Justice Award for Public Service.

The Accountability Gap and Homeland Security: Are Our Supervisors Ready?

David Hudson

Since September 2001, we have known that all levels of law enforcement—local, state, and federal—will be called upon to take critical new roles in the Homeland Security effort. As we feel our way, we will discover the nature of this new task of protecting our communities from a shadowy, global enemy whether it operates abroad or in our own communities. America will eventually get the job done. We are a people who, when called upon, can act swiftly and effectively. We will make mistakes, certainly, but we always seem to learn how to take care of business when we have to.

Over the past 25 years, law enforcement leaders and rank and file alike, have raised the bar of professionalism, year after year. This has happened across the board in the areas of training, technology, equipment, systems, ethics, job knowledge, and community-oriented service delivery.

Since the New York-Pentagon strike, the stakes have been ratcheted up another notch. We still have the usual workload we had before, *plus* we must now develop a reasonable response to the new threat to our homeland. Undoubtedly, police agencies will adapt and do what needs to be done. Our police professionals are patriots, and they are optimistic. They say, "Sure, bring it on . . . we'll handle it. It's what we do!"

But, are our supervisors ready for this additional new job?

In many ways, our supervisors *are* ready. There is no shortage of patriotism and courage in the supervisory ranks of American policing. As we witnessed in New York City, if a local crisis occurs, they will be there to do the dangerous, difficult jobs that they are called to do.

Yet, as we traverse this new, unchartered territory (of homeland security and global terrorism), we will be foolishly naive if we ignore the "accountability gap."

What is the "Accountability Gap"?

The *accountability gap* is the secret that everyone knows about and very few will discuss. Your agency is a victim of this common dysfunction if you see the following things happening around you:

- Supervisors give good ratings to problem employees . . . and get away with it.
- The same problem employees remain a danger and an embarrassment year after year (the perpetual 10% taking 90% of the supervisor's time).

- Managers give good ratings to supervisors who don't take effective action to correct problem employees.

- You can't remember the last time an employee was disciplined for continual sloppy, incomplete reports, or for not responding to calls in a timely manner, or for being repeatedly disrespectful to a supervisor or coworker, or for not taking a report when one was required, or for no self-initiated arrests, etc.

- You hear in the hallways, "It would take an act of Congress to fire a problem employee around here . . . Can't be done!"

- You hear comments like, "Oh, that's just old Herb. He's always been a slug . . . Live with it."

- Evaluations are seen as a joke because everyone gets a "satisfactory" or better evaluation regardless of their performance.

- Supervisors and managers remain so inconsistent in directing and evaluating employees that meaningful accountability remains only a dream.

Okay, but these are government jobs . . . aren't supervisors and managers truly helpless when push comes to shove with a disruptive or lazy, do-nothing employee?

Actually, no! Not at all! Don't believe these myths of helplessness! We have told each other such lies for so long that we have developed an unquestioned belief in our own powerlessness. Now, by some estimates, over 90% of our first-line supervisors admit that they give up on trying to correct problem employees and eventually look the other way. They (first-line supervisors) say that they have "no support from above," so there is no point in trying. (And, since we let them get away with it, they can only conclude that "it must be okay.")

Nowadays, supervisors erroneously claim helplessness, and those claims go unchallenged. Consequently, a whole generation of employees knows that performance is optional—that good work and poor work pay the same.

Here is the obvious truth . . . the truth that everyone knows: **Problem performers exist because managers and supervisors allow them to exist.**

But why worry about it now?

After 40 years of dogmatic, politically correct emphasis on employee rights and employee relations, law enforcement leaders across America are beginning to awaken to the fact that managers' rights and the employees' obligation to perform have been dangerously neglected.

Sadly, in law enforcement agencies, as in most other American work places, the usual supervisory role-modeling is of the "give-away-the-store" variety of leadership; in other words, the "human-relations-techniques-with-no-teeth" variety. Such organizational flabbiness is now seen as the norm. Instinctively, we all know this is not good enough to see us through the challenges ahead. We know

in our hearts that human relations techniques have serious limitations, and that a tougher, results-centered style will have to emerge.

An improved agency work ethic will not come about through taking the path of least resistance, nor will it come about through consensus of all employees. The real leaders in law enforcement will be those who assert performance standards that are appropriate for the complex policing tasks of our time and who then make their managers and subordinates accountable.

We will not find this new, "directive" style of leadership discussed in our halls of learning, in our academies, or in current-day textbooks. Does that mean that this new style is wrong? No, it means that the textbooks are naively blind to the fact that leadership without teeth (accountability) is only cheerleading. Again, cheerleading is not good enough for police work in the 21st century.

Some Suggestions to Chief Executives

I. Make a card to keep on your desktop. On the card put, "90%" in bold print. This will stand for 90% of America's supervisors. These are the ones who fail to correct problem employees. Also, keep in mind the 90% of managers who allow supervisors to look the other way and give good ratings to problem employees.

II. Make another card with a "to-do" list of unpleasant, but important things to do.

The list should contain executive actions such as the following:

1. Figure out a way to specify to the department what I expect. Do this in specific terms for each position in the department. (Find out about performance standards!) Make getting the real work done a top priority from the Chief's office."

2. Make performance evaluations meaningful in the department.

   - Stop evaluating personalities.

   - Start evaluating the actual work delivered by officers, dispatchers, etc. (Don't laugh. Performance-based appraisal does not mean *quotas*! Performance-based appraisal is already being done in some agencies! Find out how they do it.)

   - Find a labor attorney with guts—one who is comfortable with the *day's work for a day's pay* concept—and who knows how to make permanent employees accountable for meeting reasonable performance standards.

   - Say to the next in command, "Commander, if your people meet the performance expectations we have set for the department, you will get a good evaluation. But, if you have people who do not meet expectations, and you and your supervisors do not take proper and essential steps to correct them, you will get an unsatisfactory rating, and you will be placed on a performance contract."

- Sit down with one of my first-line supervisors who currently has a known problem performer. Include the supervisor's managers. Make a plan to either correct the problem employee's performance or, if that fails, through use of a fair performance contract eventually dismiss the employee.

- Sit down with the executives, administrators, and elected officials for whom I work, and their HRD experts. Enlist their support in achieving reasonable accountability. Ask them to help me send a message to all my good officers and employees that the good work they do is important!

Isn't this pie-in-the-sky wishful thinking?

Wishful thinking? Not at all. Others are succeeding. If the achievement of reasonable accountability for all employees appears too difficult or too revolutionary, then, step back and consider: "What is my alternative? Should I continue to compensate for and to justify the 10% who are killing us? Should I really continue to gamble that nothing really bad will happen?"

Real leaders everywhere, in spite of all the current and popular myths of supervisory helplessness, are biting the accountability bullet. Their employees are thanking them for it. Police work and homeland security are too important to do otherwise.

So, as the man said (high above the Pennsylvania landscape that fateful Tuesday morning in September), "Let's roll!" There is no time like the present.

David Hudson, Director of Marin Consulting, Saint Helena, CA has trained over 9000 law enforcement supervisors and managers from hundreds of agencies in the U.S. in accountability techniques that are consistent with both labor law and the human relations values of our time. Dave has published a number of articles about "The Accountability Gap" in police journals and magazines and has presented his message at IACP conferences and several State Chiefs' and Sheriffs' Conferences. Hudson urges police leaders to place the performance assurance job back on the shoulders of first-line supervisors and make them accountable for doing it. He has also published a self-study program for police supervisors and managers showing agencies how to achieve greater accountability; as well as a compact disc that instructs departments in creating the kind of performance-based evaluation that is so critical in achieving reasonable accountability. Dave cautions, "Leadership without accountability is only cheerleading—and that's not good enough for police work." Dave welcomes feedback on his articles. Send the positives or the negatives to him at <hudsond@napanet.net>.

Homeland Security: How It Affects Local Governments

Jim Cimarossa
Assistant Chief of Police
Springfield, Illinois

Terrorism threatens a society by attempting to instill feelings of fear and helplessness in its citizens. Terrorism is intended to intimidate or coerce civilian populations, influence the policy of governments, and hold a society or government hostage through perceived fear. Free and open societies provide an easy target for a well-directed terrorist organization dedicated to the destruction of that society. In the wake of events of September 11, 2001, the lives of Americans have changed drastically—being transformed from complacency to an environment where our lives and the economy are now being threatened. Preparations for disasters have been given the highest priority, and guarding against terrorist acts is recognized as a critical need. Local governments have always depended on assistance from federal level agencies in protecting our air, water, food, utilities, communications, emergency services, and transportation systems from a wide array of possible attacks. Today, city managers and mayors of local governments are forced to find additional resources and provide strategies to ensure the safety of their citizens.

Growing public attention from domestic terrorism in the new millennium has changed its focus to a more terror-causing potential involving a variety of unconventional weapons. Weapons of mass destruction that have the potential to kill large groups of people and create mass fear with the public are what face local government in today's society. Although threats of chemical, biological, and radiological weapons have always been threats within the international and domestic communities, new sources of unconventional weapon threats such as cyberterrorism, which is the physical attack on local infrastructure (e.g., electric power, telecommunication, banking and finance, gas and oil and transportation) are a source of concern. Another subset of this threat is terrorists' use of computers and the Internet. Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, recruit new members, and communicate securely. According to an American Water Works Association security advisory dated November 5, 2001, "cyber protests and hacktivist activity have increased since their September 17th advisory was issued," and the potential for hackers targeting organizations has risen since September. Contamination to food sources and supplies, also known as agroterrorism is a new and emerging threat that has required the law enforcement and public health communities to continuously improve their coordination and vigilance. This shift in focus is placing significant demands on local government resources which is requiring them to become more arduous in enhancing their capacity to respond to complex infectious disease threats, including outbreaks that may result from bio-terrorism.

The events of September 11 shocked our nation and forced local governments to consider how we should transform the way we examine our security and/or resources. At this time, existing local government emergency preparedness

plans are being examined for efficiency and effectiveness. Efforts to strengthen comprehensive emergency management plans have redoubled, and there is new consideration of how police and other public safety resources respond, illustrating just how concerned officials have become about the nation's preparedness for a bio-terrorism attack. This is occurring at significant additional cost to local government budgets at a time when tax revenues being generated by local economies is dropping. This combination of an already weakening national economy, job layoffs, consumer anxiety created by the recent terrorist attacks, and rising public safety and security costs now threatens the solvency of local governments throughout the nation.

Local Initiative

To deal with this situation, every U.S. city must improve security while constantly making changes to anticipate future terrorist activities. As a result, the City of Springfield, Illinois formulated the Office for Hometown Security which is responsible for the policy development and coordination of all security activities relating to extraordinary events within the City of Springfield, focusing on threat assessment, prevention, and preparedness. This will require working directly with local governments and coordinating their leadership initiatives to help ensure the safety and security of local communities. In addition to coordination of security for the city, the Hometown Security Coordinator is also responsible for coordination with the fire department and public health officials ensuring that a strong and flexible public safety and health infrastructure is in place to best defend against any public safety disaster, disease outbreak, and pandemic or domestic terrorist attack. This means that public safety and health organizations should be the lead agencies in any public health outbreak that may occur; however, it will be the responsibility of the hometown security coordinator to ensure overall communications and coordination with all city entities.

Office of Hometown Security

The principal function of the hometown security coordinator is to gather information regarding consequence management and to provide that information to those who need it the most. The coordination will also develop a Hometown Security Response Plan, outlining critical issues of coordination of all security activities and methods of reducing vulnerabilities to extraordinary events; formulate an emergency preparedness strategy; and provide liaison with state, federal, and other law enforcement organizations.

In addition, establish a Hometown Security Advisory Committee (HSAC) to provide advisory assistance, direction, and coordination in the development of a Hometown Security Response Plan (HSRP) of ongoing extraordinary events as it relates to the City of Springfield.

- **Creation of Advisory Committee** – conduct collaborative planning meetings with the public safety, health, medical, business, and academic communities focusing on community emergency preparedness protocols that include risk assessment, detection, prevention, preparedness, containment, investigation, and clean-up of all first responding services within the city.

Additional responsibilities as coordinator of the Office of Hometown Security include:

- **Policy development** – development and promotion of appropriate prevention measures to respond to major incidents and review of existing city-wide procedures, involving the deployment of security personnel and mutual aid

- **Communications and coordination** – of all public safety and private entities as it relates to the handling of extraordinary events within the City of Springfield

- **Training** – coordination and implementation of integrated training programs focusing on cross-training, mock drill assessments, and stress management of law enforcement, fire, and rescue services along with the health and medical communities

- **Education** – expansion of community policing programs along with establishing public awareness programs for information collection and public confidence

- **Technology** – reassessment of needed equipment and supplies conducive to unconventional methods relating to domestic incidents

- **Outreach** – provision of a forum to engage with public officials, business, academic, and media communities to collaborate with issues relating to major events

- **Analytical studies** – formulation of a central information repository to analyze, inventory, and evaluate threat assessments and information received from various sources for accuracy, dissemination, and examination of technology of DNA applications

- **Funding sources** – examination of existing budgets to reflect the shifting of priorities and obtain federal funding for local governments as it relates to domestic terrorism activities

Hometown Security Response Plan

One of the responsibilities of the HSAC will be to assist in the development of a local response to the national Homeland Security effort in Springfield. The first initiative is the development of a Hometown Security Response Plan (HSRP) to include the following:

- Assess domestic response capabilities.

- What are local government priorities and responsibilities?

- Identify areas of vulnerabilities.

- Identify resources that are available and needed.

- Establish first responder protocols of planning, identification, notification, mobilization, treatment, and recovery.

- How can the local public safety and health communities assist state and federal agencies?

- Coordinate with local, state, and federal agencies

Conclusion

Law enforcement's challenges and focus have changed drastically since September 11, and the ability to counter threats from domestic terrorism will continue to grow. These challenges that law enforcement is faced with underscore more than ever the importance of improved coordination and cooperation, effective inquiries, and the conduction of thorough and aggressive investigations. Everyone must do their part. Be aware. Take immediate steps in safeguarding your infrastructures and information, both online and at home and most importantly within your communities. The cities of our nation should be reassured that all levels of governments are taking steps to provide for their safety and security. The Office of Hometown Security is the first step to be taken by the City of Springfield, in providing direct advice, assistance, and coordination to the security efforts of the entire city.

References

Barnevek, P. (1994). *Global strategies: Insights from the world's thinkers*. Cambridge, MA: Harvard Business School Press.

Gordon, J. R. (1996). *Organizational behavior: A diagnostic approach*. Englewood Cliffs, NJ: Prentice Hall, pp. 39-53.

Mintzberg, H. (1994). The fall and rise of strategic planning. *Harvard Business Review*, *67*(1), 47-62.

Jim Cimarossa is assistant chief of police for the City of Springfield, Illinois and was recently assigned the role of hometown security coordinator. Cimarossa is a 28-year veteran of the Springfield Police Department and has a master's degree in strategic management and international business. He is pursuing a doctorate in public administration at the University of Illinois at Springfield.

Radio Interoperability: Satisfying Communication Deficiencies in the War on Terrorism

Terry Mors

Effective communication is critical in the war on terrorism. Not only must law enforcement effectively communicate on a domestic level, it must now communicate on a global level. Terrorism knows no jurisdictional boundaries. Law enforcement must critically reflect on past practices and act to correct deficiencies in communications.

Since the inception of the modern paid police force, law enforcement has been autonomous. Law enforcement agencies were organized by jurisdictional boundaries. Each village, town, city, county, and state was responsible for providing police services within their respective jurisdictional boundaries. Each jurisdiction had its own body of government that included a person or persons responsible for the administration of police services. Since policing responsibilities were established by jurisdictional boundaries, law enforcement officials worked within their own boundaries. There are currently more than 40,000 police jurisdictions and approximately 450,000 police officers (Wrobleski & Hess, 2000). Organizational complexity is a problem due to the fact that there are so many various and autonomous police agencies. Departments often utilize separate radio frequencies, which inhibits communication. Effective communication is much more difficult in this environment than it would be in a national police force utilizing a common radio frequency. A proactive approach to communication between law enforcement agencies is crucial to the success in fighting terrorism. Unfortunately, law enforcement remains reactive, and that is most evident in the area of communications.

Effective communication is paramount to the success of any organization. Communication has been characterized as the "life blood" of effective organizations (Stoner & Freeman, 1992). Effective communication is necessary in carrying out the goals and objectives of any organization, including law enforcement; however, poor communication has plagued law enforcement efforts for nearly two centuries.

Radio interoperability is the one area in which law enforcement is still vulnerable.

In its simplest terms, radio interoperability is nothing more than the ability for public safety agencies to communicate effectively with one another. Now the war on terrorism is in full swing, and law enforcement is still ill-equipped to communicate with each other. The fight against terrorism is one that requires partnerships that include police, emergency medical services (EMS), and firefighters. Most public safety agencies are not able to communicate with one another. Many police, EMS, and fire departments use separate radio frequencies. That was driven mostly by jurisdictional concerns; however, we live in a global society. Crime and disaster know no jurisdictional boundaries. The most recent terrorist attacks on the World

Trade Center were examples of how several public safety agencies were called upon to act in concert with one another to save lives and investigate crime. New York City police, fire, and EMS agencies operated in conjunction with several municipal public safety agencies from neighboring towns, hospitals, private ambulance services, the New York National Guard, the port authority, county and state police, as well as several federal agencies. Radio communication was such a problem that public safety officials pleaded with local merchants for use of public radio band two-way walkie-talkie radios. Public safety agencies must be able to communicate effectively with one another.

In the law enforcement effort against terrorism, municipal, state, and federal agencies are acting in concert with one another. At times, even the military has been called in to assist. Such was the case when California National Guard troops were assigned to protect major west coast bridges from suspected terrorist attacks. All of these agencies must be able to communicate with one another. In the past, when the need arose for public safety agencies to communicate with one another, that communication was usually done through a telephone line and a series of telecommunicators. An agent from a federal agency may need to speak with a police officer from a municipal agency. If the two agencies are using different radio frequencies, that is not possible. The agent must call his or her agency, have telecommunicators call the municipal police department, and relay communication through a series of telecommunicators. Information is then passed back and forth through a series of dispatchers.

The archaic process just described is time consuming and contains potential problems. Information passed in that manner can be misinterpreted or even erroneous. Secondly, telecommunicators may miss vital air traffic while relaying messages over the telephone. Finally, it takes telecommunicators away from their initial responsibilities. That could have life threatening implications. Telecommunicators cannot put people with medical emergencies on hold while they relay messages for officers from different agencies. It may also be possible that the information being relayed by officers from various agencies is equally as life threatening. The only alternative is to partner officers from various agencies together, so they would have radios from each agency with them. That works if only two agencies are involved. When multiple agencies are involved, however, that strategy is not a viable one. Partnering officers together reduces manpower that may be better utilized elsewhere. In some larger metropolitan areas, it is common for various law enforcement agencies to interact with each other on a regular basis. With the terrorist investigation being a global one, communication will be critical but difficult if not impossible.

The solution most certainly lies in pending technology. Until the day arrives when radio systems can receive and transmit data over several frequencies, an interim solution is needed. That solution is radio patching. Radio patching allows public safety agencies utilizing various radio frequencies to communicate with one another via land-based telephone lines. There are three groups currently testing radio patching as a possible viable solution to their radio communication problems. The first is a program called the Border Research and Technology Center (BORTAC). BORTAC was born out of a request by the U.S. attorney for the southern district of California. The U.S. Attorney was seeking a cost-effective solution to radio interoperability in southern California. The U.S. Attorney turned

to the U.S. Navy Public Safety Center in San Diego and the National Institute of Justice (NIJ) in Washington, DC. The collaboration resulted in a radio patching system that allowed 16 local, state, and federal public safety agencies in San Diego County. The program has been so successful that it prompted a spin-off group called Rio Grande Communications (RIO-COM). RIO-COM is a radio patching system that connects 11 agencies including municipal, county, and state police as well as the FBI, INS, DEA, and the Customs Department all along the Rio Grande Valley south of Texas. The hub for RIO-COM is the Brownsville, Texas Police Department.

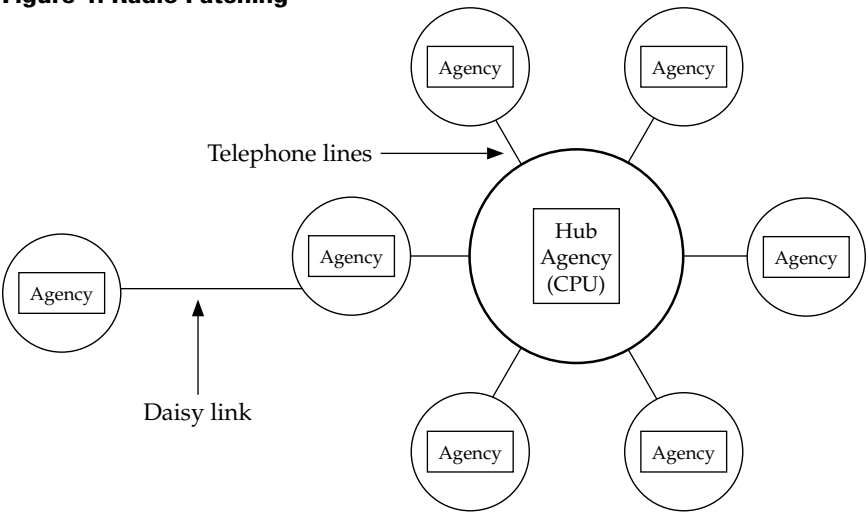
The third public safety radio patching system is an NIJ program in Alexandria, Virginia called the Advanced Generation of Interoperability for Law Enforcement (AGILE). The AGILE program was created in 1998. Alexandria police and fire departments have the ability to talk with each other as well as county, state, and several federal agencies. Given their location, Alexandria police and fire routinely interact with federal agencies. The problem was that they had no way to communicate via public safety radios due to all agencies being on separate frequencies. Alexandria is a test sight for public safety radio patching. To date, the program has proven to be very effective. While it is admittedly a "Band-Aid" solution, it is filling a current void in public safety communication.

The radio patching system is set up much like a wagon wheel with several spokes radiating out from the center. One public safety agency acts as the center or hub of the system. All other agencies are linked to the hub agencies via a land-based telephone line. The system is activated when an officer from any agency requests a patch to another agency through his or her own dispatch center. The telecommunicator from the requesting agency calls the hub agency via the telephone. He or she requests a patch to a particular third party agency. The hub agency then calls the third party agency to tell them they are setting up the patch. After that telephone call, the hub agency telecommunicator merely uses a computer mouse to click on an icon joining the two other agencies.

Radio traffic from the first officer is sent out over the airwaves to their own base station. Those voice modulations are then sent via a telephone line to the hub agency where a computer routes the voice modulation to the third party agency via another telephone line. The voice data is then dispatched out over the third agency's own radio system. The entire voice transmission takes about the same time as any normal radio transmission. Telecommunicators are then free to do their own tasks; delays in radio transmissions are minimized; and errors in communication are reduced. It is only taking a few minutes to set up the link in test sites. Once the link is made, officers from the agencies linked together can talk freely as if they were all on the same radio frequency. Low band, VHF, UHF, trunked systems, and 800 MHz systems can all be interfaced with one another. They can continue to communicate in this fashion until the link is finally broken upon request of the agencies involved.

Additional agencies can be added to the system at any time. They may be added as another spoke in the wheel, or they may connect through any of the agencies already participating in the system. Linking to an existing user is done in the same manner, through a dedicated telephone line called a "daisy link" (see Figure 1).

Figure 1. Radio Patching



The benefits of a patching system are great. First, it requires no additional new radio frequencies. That is important, as radio frequencies are becoming scarce due to increased demand. Secondly, it does not require expensive equipment. A basic interface module (BIM) is required at each end of a dedicated telephone line. In addition, there is a one-time fee for the installation of phone lines and a monthly service charge. The hub agency must also install a central processing unit (CPU) to handle the links from other agencies. On average, it has only cost agencies $2,000 to $3,000 for BIMs and phone lines. The bulk of the expense is in the hub agency's CPU. Funding for such a project can be accomplished through sharing of expenses by participating agencies, 911 surcharges, possible grant funding, or even funding from private and public donations.

Admittedly radio patching is a short-term solution. Future technology will undoubtedly offer public safety agencies better solutions; however those solutions will most likely come with a hefty price tag in the form of new hardware, software, and radio equipment. The domestic war on terrorism cannot wait for new technology to be available. Patching allows public safety agencies to communicate effectively with each other right now at an affordable price. As the war on terrorism has become multi-jurisdictional, and even global, public safety must broaden its communications abilities. Radio patching is a step towards achieving that goal.

Bibliography

Patching your way to a fix. (2000, Fall). *Tech-Beat*, pp. 5-7.

Stoner, J., & Freeman, R. (1992). *Management.* Englewood Cliffs, NJ: Prentice Hall.

Wrobleski, H., & Hess, K. (2000). *An introduction to law enforcement and criminal justice.* Belmont, CA: Wadsworth/Thompson Learning.

Terry Mors is an assistant professor with the Department of Law Enforcement and Justice Administration at Western Illinois University. He is a former instructor for the Criminal Justice Institute of Lake County, Illinois and a former police commander. Professor Mors can be reached at <Terry_Mors@ccmail.wiu.edu>.

One Terrorist Incident Demands One Technology Solution: To Bolster Community Confidence and Ensure Your Legacy

Andrew G. Mills
National TeleCrime Corporation

It took one plane to collapse each tower of the World Trade Center, one bullet to touch off a fire storm of protest, and one acquittal to devolve a community into chaos. It takes one convention to paralyze a city, one tornado to destroy order, and one crime series to suspend normal life. Terrorism, crime, natural disasters, riots, conventions, labor strikes, anarchists, abortion clinics, staffing shortages, and large conventions are some of the litmus tests a chief of police must pass in order to leave a positive legacy. This is a critical time for them to show the community that they can have confidence in the police, even in the midst of a crisis.

Adapting a comment from Reverend Martin Luther King Junior, "A man [Chiefs] is not measured during times of comfort and convenience, but during times of conflict and controversy." Most police agencies have done well to train themselves in Mobile Field Force (MFF) and disaster preparedness response, man made or natural. They are not however ready to continue routine police services. Most communities should have no expectation that police services will continue, even though their expectation is that it will. The things that give the community confidence and a sense of order during chaos are the first police services to go by the wayside.

There are three psychological desires that need to be fulfilled during an act of terror or crisis. Basic police services such as report writing and information dissemination must continue. There must be a place for people to vent and report relevant information without overburdening communications, and they must receive information and comfort from government leaders. Fortunately, the police are best positioned to fulfill this need on a local level and demonstrate to the community that they can have continued confidence in government. Unfortunately, the police are ill–prepared to perform this function.

Reducing the level of fear is critical to successful community recovery. Government agencies spend millions of dollars painting over graffiti and cleaning up litter to reduce fear, but the silence is deafening when calamity strikes. Community members want positive, personal, and compassionate service when there is opportunity for interaction. They want to report crime when it's convenient for them, normally when they call, and the ability to do their part in the effort to rid terrorists and criminals from their neighborhoods. Let's not delude ourselves into thinking the community wants a tape recorded voice message during dinnertime, broadcasting a sterile message. The police don't currently have the expertise or funding to put this into place and provide these services. There is, however, a solution new to policing, already being implemented in forward thinking police agencies and sheriff departments.

National Crime Reporting Service

Police agencies now have the ability to outsource their noncritical crime reporting function to a qualified, capable, and highly secure private entity led by police officials. Calls reaching your nonemergency telephone lines are transferred via 800 numbers to a technologically sophisticated and rapidly mobilized police support center. The calls are answered immediately, and the reports are recorded on custom software designed to capture the same information the police do. Once completed, the reports are printed on the police agency's report forms or uploaded to the record management system. The result is that the police are now free to control the crisis and respond where needed. The bonus is that the community's needs are met in an orderly and creative fashion. The community realizes that even in the midst of chaos, the police kept control, met their needs, and restored a sense of order without dropping essential services.

The Intelligence Reservoir

Shortly after September 11, I sat under a palm tree, having a drink and talking to my friend, Dave, about the events of the week. He asked if patrol officers were involved in tracking terrorists, hoping that they were arresting one terrorist after another. The reality was that we really did not have a method of collecting and transmitting data to the proper authority. Dave had some information about a person he suspected of being a terrorist. This person, as it turned out, was a Hamas sympathizer who was disillusioned with life in the United States. Unknown to Dave, the young Palestinian was the victim of a hate crime and mentioned suicide when interviewed by police. The Intelligence Reservoir is a service that can be mobilized on a moment's notice and collect data on your behalf allowing you to rapidly sort through information and focus on those who are creating disorder. Think of the thousands of people in L.A. who would have reported looters had they had the opportunity to do so in an organized, anonymous, and rapid manner. Millions of dollars in stolen property could have been recovered had a system like the Intelligence Reservoir been available.

The Community Mobilizer

Lack of knowledge is the beginning of fear. A public armed with knowledge is dangerous to the threats of terror. More importantly, a community armed with information can become a mobilized community, ready to take on the challenge of helping one another heal from the wounds of destruction. The Community Mobilizer can turn a fearful and hidden populace into a fearsome adversary ready to get personally involved. Outbound calls are systematically made to residences and businesses, encouraging calm and persuading involvement on behalf of the police. Specific scripting information allows exact messages to be sent each and every time.

Even though it takes one event to change the course of history, it takes one solution to encourage the community, bolster confidence, and perform at the highest levels possible. TeleCrime has built the infrastructure and provided the service to ensure your legacy as a police executive is not left to chance, but fortified by preparation and strategic thinking.

Each chief will face a crisis during his or her tenure. Are you prepared to handle the unexpected, yet most significant events of your tenure?

To plan for unexpected catastrophic events, call Andy Mills, National Telecrime Corporation, (858) 487-9370, or e-mail him at <amills@telecrime.com>.

Andy Mills
16981 Via Tazon
Suite B
San Diego CA, 92127
(858) 487-9370 ext. 3
amills@TeleCrime.com

Andy Mills is cofounder of the National Telecrime Corporation. He also continues to lead a team of police officers in southern California, where he has earned recognition in four Herman Goldstein awards. Andy was the year 2000 Gary P. Hayes award winner, presented to him by the Police Executive Research Forum for "outstanding initiative in improving the quality of police service."

Terrorism and Identity Validation Using LocatePLUS

Russell Slam
Director, Sales and Marketing
LocatePLUS

September 11 has shown that there is an overwhelming need now for all sectors of our economy and governments to have a better way to confirm identity. This means more than just seeing people's licenses to confirm that they are who they say they are.

"Identity Validation" is now becoming critical because of the ease with which false identification can be obtained and with the huge and growing incidences of identity theft—over 500,000 cases last year.

But the problem is "How do businesses such as airlines and security firms authenticate the identity of thousands or perhaps tens of thousands of people a day?"

First, there needs to be some method to decide which individuals need to be identified. With airlines, all passengers must have proof of identity, but how does the person issuing a ticket or a boarding pass decide which individuals need to be checked more thoroughly? In most cases, if an individual has gone to the effort to falsify identity, his or her name is not going to show up in any criminal databases like the NCIC. The identities of such individual's needs to be checked in public records and what the checker needs is a database that can identify virtually every adult in the country.

How would this work? LocatePLUS is just such a database. It is a web-based service, easily accessed and able to give instantaneous background information on a wide range of variables.

Each LocatePLUS record or report includes an individual's name, aliases, social security numbers, present address and previous addresses, current and previous telephone numbers, others living at the current address, month and year of birth (including that of other people on their report), neighbors with phone numbers and addresses, real estate holdings, drivers' license information, death records, and liens and judgments.

All of this information is available immediately. How would the security checkers use this information? They would use it as a step to further screening of the individual.

For example, if there were no record on the individual, this would immediately draw suspicion. If the age of the individual on the report did not coincide with the person's apparent age, this would be cause for further interrogation. A person with no previous addresses could be a cause of suspicion.

Questions can be asked of the person: What was your previous address?, What is the month of your wife's birth?, Who are the other people living at your residence? These questions and many more can be asked randomly so as not to allow the individual to prepare set answers.

How long would this process take? Very possibly a minute or less. In some cases, such as transportation, passengers can be screened at the time a ticket is purchased. If a suspicious report comes up, the passenger and his or her luggage can be singled out for further inspection at the time of the flight.

It may not be necessary to ask every person entering a building or boarding an airline. Profiling can be used as a way not to develop queues of people. Profiling can be used to eliminate certain classes of people—the elderly, frequent travelers, or recognizable tenants of buildings.

Also, in the case of transportation, lists of passengers can be run before boarding to identify potential people who should be screened in more depth or whose luggage should be singled out for inspection. LocatePLUS, in a separate service, is also able to provide large scale background checks if provided with names of people from some target group of people.

For those in law enforcement, the ability to develop lists of neighbors at a click can be a powerful tool to canvass neighbors.

What the issue comes down to is how people can be quickly identified and profiled separately from identification which they provide. LocatePLUS provides an inexpensive solution to this problem and others in which the category of people needing to be identified is part of the general population.

Russell Slam, a graduate of Pennsylvania State University with degrees in history and economics, did graduate work in economics at the University of Wisconsin. He worked for ten years with Warren Gorham & Lamont, a subsidiary of West Law that publishes tax and accounting compliance information. Slam is now Director of Sales and Marketing at LocatePLUS.com, a leading civil record data provider of web-based investigative databases located in Beverly, MA.

Identity Theft and Online Crime Workshop Panel Hosted by the IACP 108th Conference, Sponsored by the IACP Criminal Justice Information Systems Committee and the National White Collar Crime Center

Steve Edwards, Special Agent, Georgia Bureau of Investigation

Introduction

On Tuesday, October 30, I had the pleasure and honor of moderating a panel entitled "The Fastest Growing Crime in The Twenty First Century" for the International Association of Chief's of Police in Toronto, Ontario, Canada. The panel addressed issues for the local and state criminal justice community related to identity theft and online crime. I had the distinct pleasure of sharing this panel with some very talented and capable people from across the U.S. with many years of law enforcement and investigative experience.

Robert Zidek, chief of police for Bladensburg, Maryland, who has 45 years experience in law enforcement with most of that time spent as a chief executive officer, discussed how a small department could investigate identity theft. It was at the St. Louis Economic Crime Summit, hosted by the National White Collar Crime Center, back in 1998 where I first learned of Chief Zidek's program. I was impressed with it, and as a result, I returned to my own state investigative agency and instituted some changes to assist victims of identity theft.

Reid Wittliff, internet bureau chief for the Texas Attorney General's Office, one of the most proactive online crime investigative units in the country, discussed how Texas is handling online cybercrime especially in the area of identity theft. Wittliff went into great detail describing programs implemented by various local and state agencies in Texas through partnerships to deal with online crime, including computer forensics.

Phil Ramer, special agent in charge for the Florida Department of Law Enforcement's Statewide Intelligence Squad, discussed how Florida is dealing with identity theft. Ramer also discussed how some of the suicide terrorists from the September 11 attacks had lived and acquired identification materials in Florida including drivers' licenses.

Bob Berardi, a detective sergeant with the Los Angeles County Sheriff's Department assigned to the Southern California High Technology Task Force/Identity Theft Detail, who has been in law enforcement for 19 years, discussed how California

is dealing with identity theft. Detective Sergeant Berardi's unit is one of the most progressive identity theft investigative groups in the country.

Also on the panel was an identity theft victim from Georgia who shared her experiences as a victim. She talked in great detail about her experiences as a victim since first finding out that her husband's identity had been stolen in October 2000. She shared her stories about having to contact so many various agencies before finally getting help and ultimately having the perpetrator arrested and jailed.

Identity Theft

According to the U.S. Secret Service and the Federal Trade Commission, identity theft is one of, if not the, fastest growing crimes in the United States. It is predicted that within our lifetime, one in four of us will become a victim of identity theft. Computers and the Internet have made it easier for perpetrators to commit identity theft and go undetected. Traditional methods for stealing someone else's identity remain the form of choice, but because of databases and sites on the Internet that contain so much of our personal information, this is starting to change. More identity thefts are occurring over the Internet, especially the theft of credit card information.

Historically, victim's identities have been stolen by perpetrators doing "dumpster dives" and retrieving trash thrown out by the victim or by a business having a relationship with the victim. Of course, the perpetrator would be looking for any documents, mail, or applications with identifying information. Mailboxes are also raided by perpetrators of identity theft looking for mail containing useful information. Perpetrators have historically also taken low paying jobs such as clerks or security officers that would place them in a position of being able to obtain various identifiers related to employees, customers, and others having a relationship with the company or business. Another method has been for perpetrators to use social engineering skills. This method would entail the perpetrator contacting the intended victim and employing a scheme in which the victim would voluntarily provide his or her identifying information.

The identifiers that the perpetrator is seeking regardless of the method employed includes full name, dates of birth, social security numbers, addresses, telephone numbers, place of birth, date of death, credit card information, bank account information, relatives, as well as other personal data. When this information is collected and pieced together, it makes it quite easy for the perpetrator to obtain credit and documents including drivers' licenses in someone else's name.

Perpetrators of identity theft have been known to use the stolen identity to obtain not only credit and material assets but also to obtain a drivers' license or a job. There are documented cases in which a stolen identity was used to obtain a driver's license because the applicant had been arrested so many times for driving under the influence (DUI) that his or her real driver's license had been revoked. In a case in Georgia, the victim applied for a job only to be told that he was not being considered because he had been arrested for DUI twice in the previous year and that there was an outstanding arrest warrant in his name. The victim was able to prove through fingerprints that it was not him that had been arrested for these

DUIs. Unfortunately, by the time he went through the process, someone else had already gotten the job for which he had applied.

There are documented cases in which someone's identity was stolen in order for the perpetrator to obtain a job or conduct business. In one case, a perpetrator stole someone's identity and used it to start a health care service that had a relationship with the state Medicaid office. Of course, the perpetrator was committing fraud through the business by billing Medicaid for patients that had not received any service. The victim did not find out about his identity being stolen until IRS informed him that he owed back taxes for the income of the fraudulent health care business. By this time, the State Medicaid Fraud Control Unit was also looking for the identity theft victim for the fraudulent transactions that had been committed using his name. There are also cases in which a stolen identity has been used to obtain tax refunds intended for the victim.

Identity theft is being perpetrated by individuals as simply a crime of convenience, as well as by organized crime groups through sophisticated and complex schemes. This crime has become a national security issue in that terrorists are using false identities to perpetrate their terror. There is some concern that terrorists may have been able to enter this country by having stolen the identities of others from countries abroad. Another concern is that as identity theft continues to increase, it will affect our economy because of the burden it places on our financial and lending institutions to cover the losses.

Computers and the Internet are being used by criminals to share knowledge and information. In the area of identity theft, the criminal will often exchange victim identifiers with others via the Internet. Because of the computer media, victims are now more than ever likely to see their identities compromised by more than one perpetrator in many different parts of the world.

Identity Theft Victims

As our panel victim pointed out in her presentation, the criminal justice community is not doing a really good job in helping the victim. When victims call their local police or sheriff's department, they are sometimes told that they are not victims and not to worry about it. Other times, the victim is told that the local jurisdiction does not have venue and that the jurisdiction where the sale took place or the act was perpetrated has venue. In the case of the panel victim, that meant contacting agencies in Colorado, Iowa, Alabama, South Carolina, and Georgia. When she contacted the out-of-state jurisdictions, she was instructed to contact her local agency that had already told her to contact them. The panel victim contacted several federal agencies only to be told that her crime did not meet their threshold in terms of loss. She went as far as to write her congressional delegation with her dilemma. One of her senators responded back that it was a state issue, and there was nothing the federal government could do for her.

From the panel presentations, especially the victim presentation, it is obvious that a system needs to be devised that allows victims to report the theft of their identity one time. Once the victims file their complaints, the information would then be forwarded to the appropriate law enforcement agencies that would have an interest in the case. Unfortunately, when someone's identity is stolen, he or she

not only must report it to the appropriate criminal justice agencies, but also to each of the three credit reporting agencies; all of the financial and lending institutions that they have a relationship with; plus any financial, lending, or other institution that the perpetrator established a relationship with through the stolen identity. As the victim from Georgia said, this can take weeks, even months to accomplish. The Secret Service has described identity theft as the two-and-a-half year crime meaning that it takes victims about two and a half years to restore their good names. As for the panel victim, she is still trying to restore her and her family's good name. She is still getting calls from lending agencies stating that she or her family owe money for debts incurred by the perpetrator in her husband's name. In addition, her husband has been instructed to keep a police report with him at all times to prove that his identity has been stolen to prevent him from being arrested for crimes committed by the thief.

National Database for Identity Theft

The Federal Trade Commission (FTC) has developed a national database for identity theft victims to report their crime known as the Consumer Sentinel. The victim can report the theft of identity at (877) 438-4338 or via the Internet at <www.consumer.gov/idtheft>. Any recognized law enforcement agency through a Memorandum of Understanding (MOU) with FTC can review the names in the database via computer. Unfortunately, FTC does not send these complaints out proactively to the appropriate law enforcement agencies that would have venue. It is my understanding that the Secret Service has detailed a special agent to work with FTC on this project so as to make this program more proactive. Another draw back is that this information can not be shared with the credit reporting agencies or any other appropriate private entity such as financial and lending institutions.

According to the FTC, between November 1999 and June 2001, 69,370 complaints were filed by consumers. Fifty four percent of those complaints received by FTC had not been reported to the police. Of the complaints that had been reported to the police, the police failed to file a report for 28% of those reported.

The National White Collar Crime Center through a partnership with the FBI operates the Internet Fraud Complaint Center (IFCC) on behalf of local and state criminal justice agencies. Through IFCC, a victim can report a crime via the Internet. IFCC was specifically set up to accept Internet fraud complaints including identity theft over the Internet, but victims are using it to report all types of crime. Since the September 11 attacks, IFCC has been accepting information related to the attacks and terrorism via the Internet.

IFCC is proactive in that every complaint received that is completely filled out is provided to the appropriate law enforcement agency having jurisdiction. Each agency that receives the complaint is provided with a list of the other agencies that received the same complaint so the investigation can be coordinated between agencies. Between July 2001 and before the September 11 attack, IFCC recorded 15,162 complaints. Unfortunately, IFCC also does not have a vehicle in place through which the credit reporting agencies, financial institutions, and lending institutions can access this information.

Several private interests like the credit reporting agencies, financial institutions, and lending institutions have expressed an interest in having the ability to access a national database related to identity theft. These same institutions have reported that if they had a mechanism, they could report through to criminal justice agencies around the country and they would be able to provide lead information related to identity theft. According to some of these companies, they have inhouse programs that identify potential fraud as it is happening. These companies say that with the appropriate safeguards in place, they would be willing to share this information with law enforcement alerting potential victims and making apprehension of perpetrators much quicker.

Public Awareness

One of the big issues related to identity theft is making the general public aware, as well as the business community. Georgia has taken this task on through a partnership known as the Stop Identity Theft Network. Created in the fall of 2000, the partners include local and state government as well as the business community. Through this partnership, the panel victim was able to get some action taken toward solving the crime, and in fact, the perpetrator is now incarcerated.

Through town hall meetings across the state, the message about identity theft is getting out in Georgia. As a result, law enforcement has taken some new approaches to dealing with the issues. These approaches include additional training for law enforcement personnel including sworn officers, as well as 911 operators. The Georgia Crime Information Center recently sent out a special operations bulletin to every terminal agency operator addressing identity theft and what a victim should do. The bulletin encourages local agencies to complete an incident report when identity theft is reported. In addition, a page on identity theft has been added to the Criminal Justice Information System manual which outlines what victims should do when their identity is stolen. The Special Operations Bulletin is attached as Appendix One.

Through this network, Georgia has proposed partnering with the IFCC for Georgia residents to report identity theft. If the proposal is accepted by the National White Collar Crime Center, links will be established at various Georgia websites including the Governor's Office of Consumer Affairs, the Attorney General's Office, and the Georgia Bureau of Investigation with IFCC. When the victim opens the link, the form he or she completes will reside on the NW3C servers in West Virginia, but the page will appear to be in Georgia. The page will have the state seal and other state identifying information. When the complaint is completely filled out and submitted, the victim will receive a digital response through a letter signed by the Georgia Attorney General thanking the victim and providing him or her with additional information as to what should be done next. Through IFCC, the complaint will then be forwarded to all of the appropriate criminal justice agencies in Georgia, as well as any other effected jurisdiction across the country. As with all IFCC complaint disseminations, the receiving agencies would be provided with a list of other agencies that received the complaint so investigations can be coordinated.

Another project that the network has taken on is the development of an identity theft questionnaire form that will be used by all agencies in Georgia to take

a report of identity theft. This report would be used by both government and private entities when taking a complaint related to identity theft. The proposed questionnaire is attached as Appendix Two.

Investigators of Identity Theft

Any competent investigator can conduct investigations of identity theft. The more training the investigator has in financial investigations, all the better, but the reality is most of what an investigator has to contend with in identity theft investigations can be overcome with good old fashioned police work. Of course, the better the investigator understands the *modus operandi* of the identity thieves, the easier for the investigator to piece the investigation together.

Investigations Involving Computers

Investigations that involve computers, including identity theft for which a computer was used, require more skill set for the investigator. While these skills and knowledge will not replace good old fashioned police work, they are tools that the investigator must possess in order to conduct the investigation successfully. These skill sets include the knowledge to trace an e-mail to the server or Internet Service Provider (ISP) from which it originated, to locate the server or computer on which a web page resides, a newsgroup resides, or a chatroom resides. The investigator must possess the knowledge to discuss these issues with the prosecutor, the ISP, and others. This knowledge includes the ability to articulate what evidence they are looking for through search warrants and subpoenas.

The investigator also needs the knowledge and skills to seize computer evidence without jeopardizing the integrity of the evidence and making the evidence inadmissible in court. These days, the only evidence that the investigator will have will reside on computer media and the servers of the internet provider. In addition to possessing these skills, the investigator must also have the availability of computer forensics or have these skills him- or herself.

Computer Forensics

Once the computer media is seized, the investigator will either have to conduct computer forensics or have someone conduct computer forensics to extract the evidence. To ensure that the evidence is not tainted, a bit-by-bit stream of the suspect media must be imaged. This is not like creating a backup image, because every bit is copied from the targeted media due to hidden data and documents on computer media that even the central processing unit (CPU) does not recognize. This technique captures erased and deleted files, partial files, crossed files where text or other data remains in a sector after the file has long since been deleted and a new file has been placed in that sector by a CPU, and slack space where a suspect has added a file or data to a sector not recognized by the CPU without certain utility software.

For investigators and the criminal justice community to investigate and prosecute these cases in which a computer or the Internet is being used to either perpetrate the crime or store evidence of the crime, certain training must be provided. To train and equip one investigator in computer forensics and investigations with

state-of-the-art technology and skills costs approximately $37,500, plus frequent updated training to ensure that the investigator remains current.

To train and equip one forensic computer specialist in a lab costs approximately $84,800, plus the cost to provide him or her with frequent updated training. Unfortunately, this training is not easily accessible to local and state law enforcement. The good news is that the training is available through groups such as the National White Collar Crime Center, the National Cybercrime Training Partnership, SEARCH, the FBI, and others at little or no cost except for travel, meals, and lodging. The bad news is that there are only so many slots available, and few agencies can afford the luxury of sending personnel away to be trained for more than a few days.

The average training is broken down into week modules, and it takes a total of eight weeks to get the investigator at the skill level desired. Because the technology is constantly changing, the equipment used to conduct computer forensics including software must be updated at least every two years. The cost for the hardware and software needed to conduct forensics on a stand-alone machine in a computer forensic lab is approximately $15,000. Ideally, a high-tech classroom should be located adjacent to the computer forensic lab so that investigators and others do not have to leave their area or state to be trained. With the classroom being part of the computer forensic lab, you can operate like a teaching hospital allowing certain students to have hands-on experiences with the classroom training. The cost for the high-tech classroom is approximately $428,000; this would include construction cost, the furniture, and the equipment. It does not include the rent or building and land.

Conclusion

It is clear that local and state criminal justice agencies have a lot of challenges ahead in addressing identity theft and online crime. Based on the presentations at IACP, it is also clear that there are many agencies out there that are using their existing resources and addressing these challenges. Additional funding and partnerships with the NW3C, FTC, and others will go a long way in helping local and state agencies meet these challenges.

Identity theft is a different crime than we have had to face in the past because of the effects it has on the victim. There is not a one-stop shop available to victims that will rid them of all the problems they face because of this crime. A coordinated effort by the criminal justice community to develop and provide a vehicle through which the victim can report the crime and know that through this vehicle all of the appropriate agencies are being notified would go a long way in bringing the victim satisfaction. Additionally, the criminal justice community developing a partnership with the appropriate private sector entities, such as the credit reporting agencies, financial institutions, and lending institutions, would also remove a lot of barriers currently faced by both law enforcement and the victim. Through this partnership, perhaps a national database could either be built or retooled within IFCC and the Consumer Sentinel that would allow information from the private sector to be inputted and accessed.

As taxpayers we all have a right to expect certain things from our governments at all levels. One expectation is that when we are a victim of a crime, we can contact our local police, report it, and at least obtain a police report memorializing the crime. Most of us hope that an attempt will be made to investigate and identify and arrest the perpetrator. Unfortunately, in regards to identity theft neither the former or latter expectation can be counted on. Hopefully through awareness programs and training, local and state law enforcement will recognize the issues and challenges for both the victim and the criminal justice community in dealing with identity theft and online crime.

Appendix One

GCIC Operations Bulletin 2001-30

Subject: Identity Theft

Effective: Immediately

Contact: Marsha K. O'Neal
CJIS Operations Program Manager
Phone: (404) 244-2846
E-mail: marsha.o'neal@gbi.state.ga.us

1. Identity Theft is a critical issue that violates an individual's privacy and adversely impacts consumer confidence in the business community. Government and business leaders in Georgia realize that in order to stop identity theft activity, members of the political, legal, law enforcement, and corporate communities must cooperate and mutually confront it. As a result, the Stop Identity Theft Network was formed. See the attached, "STOP IDENTITY THEFT NETWORK" paper.

2. The Stop Identity Theft Network will host several town hall meetings to promote public awareness for consumers, businesses, and law enforcement. For more information about the Stop Identity Theft Network or the town hall meetings, contact Javoyne Hicks, Assistant Attorney General, at (404) 651-9340 or <Javoyne.Hicks@law.state.ga.us>.

3. Law enforcement agencies are encouraged to complete an incident report (or miscellaneous incident report) when identity theft is reported. Enclosed are some suggestions on how to deal with identity theft. We encourage you to give this form to victims of identity theft.

4. Approved _____ 10/01/01
Paul C. Heppner, Deputy Director for GCIC Date

Attachments

Identity Theft: What do I do?

Effective July 1, 1998 it is a felony in Georgia to use someone else's identity to obtain something of value (**O.C.G.A. 16-9-120** through **16-9-127**).

1. **The first thing you should do is contact your local police department or sheriff's department to report the theft of your identity.**
   a. Explain to them how your identity was stolen.
   b. Provide them with copies of statements or other documents that you have that support your contention (i.e., information on bank accounts, last known information on accounts).

2. **Contact the Federal Trade Commission and the Georgia Office of Consumer Affairs (OCA) to report the theft of your identity.**
   a. Contact OCA at (404) 651-8600 or (800) 869-1123 or at <www.ganet.org/gaoca>.
   b. Contact FTC at (877) 438-4338 or at <www.consumer.gov/idtheft>.

3. **Contact the major credit reporting agencies, and have a fraud alert placed on your credit report.**
   a. Equifax, P. O. Box 740250, Atlanta, Georgia 30374-0250; (800) 525-6285
   b. Experian, P.O. Box 1017, Allen, Texas 75013; (888) 397-3742
   c. Trans Union, P.O. Box 6790, Fullerton, California 92634; (800) 680-7289
      (1) After making telephone contact with the credit reporting agencies, follow up with a letter.
         - In letter form, explain to each credit-reporting agency that someone has stolen your identity to obtain credit or for whatever reason (i.e., driver's license etc.).
         - Give factual information including copies of statements, other documents, and police reports that support your contention.
         - Include in the letter that credit should not be granted unless you or your spouse are contacted for verification.
      (2) Request a copy of your credit history.

4. **Contact the company(ies) that has provided credit or other intangible or tangible property to the person who stole your identity.**
   a. In letter form, explain that you either did not make the charges that are on your statement or that you never requested credit, or you never applied for the item(s) that were issued using your identity.
   b. Give factual information including copies of statements or other documents that support your contention.
   c. Include a copy of your police report.

Stop Identity Theft Network

Identity theft can have a devastating impact on an individual's personal and professional life or on a corporation's revenue and good name. In addition, the speed and technological advances that we take for granted have complicated this issue, and we must recognize the magnitude in order to **STOP I.T.**

In September 2000, government and business leaders in Georgia met at an identity theft conference. Those who attended the conference recognized that identity theft is a critical issue that violates an individual's privacy and affects consumer confidence in the business community. They also realized that in order to stop this criminal activity, it must be addressed by members of the political, legal, law enforcement, and corporate communities, including the financial institutions and credit reporting agencies. As a result, the Stop Identity Theft Network was formed under the auspices of Georgia Attorney General Thurbert Baker.

This organization brings together local, state, and federal law enforcement, local and federal prosecutors, corporations, and the financial institutions in an effort to educate the public and businesses, provide training for law enforcement, and establish a centralized database for victims to report identity theft. The network wants to send a strong message that identity theft will not be tolerated in Georgia.

In order to combat this issue, we must all work together to **STOP I.T.** now**!**

For more information, contact . . .

R. Javoyne Hicks, Assistant Attorney General, (404) 651-9340;
Javoyne.Hicks@law.state.ga.us or Gail Griffith, Deputy CISO, (404) 715-6045;
Gail.Griffith@delta-air.com

Appendix Two

Identity Theft Victim Questionnaire (Draft)

1. Victim's Name, address, and contact numbers. Try to verify whom you are talking to with Cris/Cross, home address, etc.

2. When did you discover something was wrong? How were you contacted, and who contacted you? (i.e., bank or credit card representative)

3. Establish venue/ all that apply.

4. What information is being used? (i.e., name, social security number, date of birth, address, phone numbers, etc.) How is your credit being used? (i.e., bank accounts, credit cards, auto loans, auto titles, utilities, cell phones, etc.)

5. Are there any suspects identified in your case? If so, are you familiar with any of the suspects? If so, how?

6. Do you have any idea how your information was compromised? Have you done any of the following recently:
   a. Traveled?
   b. Purchased anything over the Internet?
   c. Joined any clubs?
   d. Enrolled as a student?
   e. Been to the hospital or doctor's office?
   f. Filled out any type of application(s)? (i.e., credit, apartment)

7. What is the total amount of your monetary loss? Has your bank and any other institution had you file fraud affidavits? Reimbursed you? Do you have any contacts with the bank or institution? (i.e., names, contact numbers)

8. Can you provide a list of known businesses where fraudulent activity has occurred and a contact person and number for those businesses?

9. Can you provide a list of fraudulent addresses used? (i.e., used in fraudulent deliveries, contact for suspect using your information, etc.)

10. Have you contacted each of the three major credit reporting agencies to issue a fraud alert on your reports and to see if any additional activity is reported? If your social security number was compromised, have you contacted the IRS and the social security office?

11. To your knowledge, had any false credit applications been approved, or have there only been inquires on your report?

After gathering all of the information, have the victim file a complaint with the Internet Fraud Complaint Center at <ifccfbi.gov> and with the Federal Trade Commission at (877) 438-4338 or <www.consumer.gov/idtheft>. Also, provide the victim with all three major credit reporting agencies' contact numbers and addresses.

Steve Edwards has been an agent with the Georgia Bureau of Investigation (GBI) since 1973 and is currently serving as special agent in charge of the financial investigations unit. Edwards has spent the last 14 years in financial investigations, health care fraud, and computer crime investigations. Additionally, he spent six years in polygraph, three years in field investigations, and five years in narcotics investigations. Edwards is certified and trained as a polygraph examiner, fraud examiner, police instructor, and police manager. He is also trained and experienced in forensic computer data recovery. He is a former crisis negotiator for the State of Georgia's SWAT Team and is Georgia's State Coordinator to the U.S. Treasury's Financial Crimes Enforcement Network. Edwards is on the executive board for the Georgia State Computer Crimes Task Force, the board of advisors for Kennesaw State University's Southeastern Cybercrime Institute, and the board of advisors for the Information System Forensic Association. Edwards is also a committee member on the State of Georgia's Stop Identity Theft Network and a portfolio member on the National Cybercrime Training Partnership's State and Local Portfolio. He also serves on the FBI's InfraGard Watch and Warn Committee. A board member for the National White Collar Crime Center (NW3C) since November 1997, he currently holds the office of vice chair, and represents the southeast region, which includes the states of West Virginia, Kentucky, Virginia, Tennessee, North Carolina, South Carolina, Georgia, and Florida as well as Puerto Rico and the U.S. Virgin Islands. Edwards attended Dekalb College and Georgia State University and received his degree in criminal justice.

Your Terrorist Incident and the Media

Rick Rosenthal

The terrorist attacks on September 11 have forced police departments (and all other agencies of public safety) to rewrite their play books on how to manage critical incidents. For the best practices police departments, that overhaul includes a review of existing policies and procedures concerning media relations in a crisis. The best-practices agencies of law enforcement understand that the mass media—especially in times of crisis—are not the enemy; in fact, the media can be one of your biggest assets. In times of crisis, there is one way, and only one way, to get your essential messages to the public, and that is through the media.

Adopt the attitude that the media are your single biggest force multiplier, and you're way ahead of the game. But that's just your key starting point: Working with the media and getting them to work with you in any high-visibility terrorist or other critical incident is absolutely essential, but how do you achieve that mission-essential goal? That's where media relations training comes in. "Training is more important than ever," says New York Police Department Commissioner Bernard Kerik, and that should include training for media management. If your crisis preparedness plan does not include preparations for handling the media, you're not ready; there's a hole in your preparedness plan big enough to drive a fleet of TV trucks through, and you're going to end up as roadkill.

The first critical step in preparing for media relations in a terrorist or other crisis incident is to get an information specialist onto your team. First and foremost, every agency of law enforcement large and small must have someone designated to perform the public information function. A full-time Public Information Officer (PIO) slot is best, but if yours is a small agency (most are) with a limited budget (that's universal, these days), then select someone to serve as PIO part-time. Let him or her perform their "normal" duties day-to-day and fill in as PIO on an as-needed basis; just remember, in a terrorist or other critical incident, a PIO will be needed.

Who should you pick an as your PIO—a cop who can learn media relations? An ex-newsperson who can learn policing? A corporate public relations person? A total outsider? "The answer is, 'Chief, who do you trust?"' says Jim Vance, who teaches media relations at the FBI National Academy at Quantico, Virginia. Vance explains, "Absent your trust there's not a damn thing any PIO can do. If you trust someone and are willing to devote the time, let them have a learning curve, you're going to have a better public information officer regardless of where they come from. That said, I don't think it makes any difference." Vance adds, "I think people with a strong corporate or journalistic background have shown themselves to be worthwhile, because more and more agencies are going to them. On the other hand, I can understand how there may be a need for uniforms. Some organizations you get a mix of both, it depends on the market."

Once a PIO is on your team, training becomes the next essential. SGT Randy Force, media relations specialist for the Phoenix Police Department knows the value of media relations training first-hand:

> So many times you arrive in the public information officer (PIO) position, you may have been well trained in whatever field you came from, but give the PIO business its due. It is as important as any other police function or operation. You wouldn't join a SWAT team with no training; you wouldn't get on a motorcycle and enforce traffic laws without training; you should not become a PIO without getting yourself some training, hopefully before the job, but if not then certainly soon as possible.

Media relations training for law enforcement takes a number of different forms. You can learn under the FTO model from a veteran public information officer within your organization. You can also go outside your organization to other law enforcement agencies such as the FBI or the Federal Law Enforcement Training Center in Glynco, Georgia that offer media relations training. The National Information Officers Association (NIOA) offers training late each summer at its annual conference; similarly, the Public Information Officers Section of the International Association of Chiefs of Police offers extensive training each fall at the IACP's annual conference, and each spring at the section's annual mid-year conference (the next IACP PIO Section mid-year conference will be in Chattanooga, TN, April 17-20, 2002, and all are welcome.) There may also be PIO classes offered at local community colleges that specialize in law enforcement curricula, and of course, there are experienced private professional instructors who train around the country and can bring the training right to you.

What are some of the important strategies and tactics you'll learn in such training? The single biggest key to successful management of any critical incident is *planning*.

"The more you sweat in peacetime, the less you'll bleed in war," says the FBI's Vance, a retired Marine Corps colonel. "Having a strategy ahead of time is critical," he adds. That strategy for crisis management must include planning for media management.

The most basic principle of any such media management plan is that law enforcement bosses should decide right now that they will work with the media to the maximum extent possible during a crisis: regardless of the nature of the incident, you must feed the animals. In any public safety emergency, the mass media are going to be there covering the story: engagement with the media is inevitable; victory is only optional. To keep rumors and misinformation to a minimum; to inform the public of what happened and what you're doing about it; to reassure the public; to enlist help and tell your citizens what you may need them to do, you have no choice but to work with the media.

In fact, working with the media should begin long before any crisis hits. In every media relations class that I teach, I underscore the value of cultivating solid professional relationships with your local reporters and media managers—relationships based on respect, mutual trust, and mutual effectiveness. Doing so will be a huge public relations advantage to you on routine stories as well as in a crisis. Pat Camden, Deputy Director of the Chicago Police Department's Office of

News Affairs, says, "Trying to establish those relationships is the most important thing you can do. In time of need, you'll know the people you can rely on and know they'll step up to the plate and do what's required." Vance puts it this way: "Who are the 'go-to' people in the media that you can work most closely with? You'll treat them all the same, but I want to know who's got a good understanding of the whole thing, not to be a lap dog but to make sure my side of the issue is heard."

Irving, TX Police Chief Lowell Cannaday knows the value of solid media relationships. On December 24, 2000 a gang of prison escapees ("the Texas 7") shot and killed one of his officers, Aubrey Hawkins. It was an act closely resembling a terrorist incident. The media response, Chief Cannaday said, was "immediate, huge, and national." But reporters were also responsible and respectful in their coverage-- even the networks and other national media—in part because of Chief Cannaday's long-standing "open door" policy on media relations. Cannaday said, "We had always been of the feeling that maintaining a good press relationship would be invaluable to us in a time of crisis, and that proved to be so true. The press treated us with utmost respect and courtesy during the entire crisis."

Now is also an excellent time to consider drafting "rules of engagement" that you and the media agree you'll all play by in the next crisis. In Portland (OR), Tampa (FL), Boston (MA), and three other U.S. metropolitan areas, law enforcement agencies have drawn guidelines that the media have voluntarily accepted. Under these agreements, the media acknowledge common-sense guidelines for critical incident coverage, guidelines that are generally based on safety concerns; in exchange, law enforcement commits to providing the media with maximum reasonable access and support for them to shoot pictures, gather information, and report to the public in a timely manner. Live TV broadcasts and helicopter coverage are among the issues addressed in these agreements, and the media have accepted some reasonable restrictions in these areas.

Briefly, here are other basic recommendations for bosses and/or PIOs for media management when dealing with a terrorist incident or other crisis:

- Be able to distinguish legitimate media from wannabes and gawkers. At a minimum, a corporate ID that includes the reporter's photograph should be prominently displayed. Larger departments should issue their own official media credentials (with photo) once a year. During a major critical incident, larger departments should consider issuing at-scene credentials that will allow site access only to authorized media.

- Set up a media command post that gives the media an on-scene vantage point and gives you a place to hold your news briefings.

- Be accessible to the media (this is where your PIO, the one you can't afford, really earns his pay!). Remember Baltimore County PD Media Relations Director Bill Toohey's three rules of media management in a crisis: "Be there. Be there. Be there."

- Update the media as frequently as you can (at least every hour, if not more often). That was how Jefferson County (CO) Sheriff's Deputy and PIO Steve Davis handled the media at Columbine High School, and with great effect.

- Always be straight with reporters. Give them facts and information. Never speculate. "I don't know" is always an acceptable answer if it's true.

Work with other PIOs in neighboring departments to arrange for mutual aid and back-up. The Salt Lake City (UT) Police Department has undergone extensive training in anticipation of possible terrorist threats during the 2002 Olympics. Their PIO there, Sergeant Fred Louis, understands the value of having help as the department's information specialist:

> On a large event like this, mutual aid is crucial, the friendship, the bonds you've built with other PIOs. We have a state association of about 125 PIOs, I've only been PIO for seven months now, and if it wasn't for those other people helping me out, directing me, guiding me, I think I'd be at the bottom of the ocean right now. But I have had that assistance from those other PIOs. . . . You want to build those relationships the same way we do with media people. You want to build those relationships because they're the ones that are going to help you out at a big event, especially something like the Olympics or a major crime event, you're going to need the help of those people to support you. That not only makes your department look good, but it also makes the departments that they're from look good. The relationships that you build with other PIOs are important very important. Don't be the Lone Ranger at this.

A terrorist incident such an as those of September 11 will test the heart and soul any department—any officer—that's involved. The best departments and their chiefs understand the value of planning for such incidents, planning that includes a commitment to working with the media, and media training to maximize the effectiveness of the team's response. That training should be professional, and ongoing. PIOs and their chiefs "both need the same training, and they need to renew that annually," according to Bill Cheek, a retired media representative for the FBI and general chair of the IACP Section. "It's not enough to just one-time inoculate yourself against a media blitz. You've got to be able to go back and pick up the nuances, the new things, the new trends, new theories . . . . You absolutely stay on target with these training sessions."

The role of PIO "is not a job that you can just do through intuition," adds Phoenix Police Department's Sergeant Force. According to Force . . .

> There are a number of specific technical things, there's jargon, you basically have to learn the media's job. The better you understand that, the better you can help them, the better you will be at your job. And that's unlike anything that you've ever been trained to do in law enforcement before. It certainly would behoove you to get out and get as much training as you can . . . . You have to learn the business to succeed in it. You need to take the time to get training and help yourself succeed.

Rick Rosenthal is a nationally recognized media relations trainer and consultant specializing in courses for law enforcement. He can be contacted at (847) 446-6839.

Guidelines for Preparing Manuscripts

There are virtually no restrictions on subject matter as long as the material pertains, in the opinion of the editor, to law-enforcement-related areas. Manuscripts should be typed and double-spaced. A résumé or vitae from the author(s) must accompany submissions. Book reviews and research notes will be considered for publication. No submission will be published until recommended by referees, who will review blind copies.

Final manuscripts must be submitted on 3.5" microcomputer diskettes readable on Macintosh or IBM (and true compatible) computers. Please specify word processing program used when submitting diskettes (e.g., MacWrite 5.0, WordPerfect 5.1, and so on). Also, an ASCII version would be most helpful. Disks will not be returned. Figures and line drawings must be submitted in camera-ready form.

Send three hard-copy manuscripts, vitae(s), and a diskette to . . .

Vladimir A. Sergevnin
ILE Executive Forum Editorial Office
1 University Circle
Macomb, IL 61455
(309) 298-1939; fax (309) 298-2215

Manuscripts should be prepared according to the *Publication Manual of the American Psychological Association* (4th ed.) (1994). *Webster's Third New International Dictionary* (3rd ed.) (1983) is the standard reference for spelling. Contributors are responsible for obtaining permission from copyright owners if they use an illustration, table, or lengthy quote that has been published elsewhere. Contributors should write to both the publisher and author of such material, requesting nonexclusive world rights in all languages for use in the article and in all future editions of it.

Works Published/Produced Through the Illinois Law Enforcement Executive Institute

Emerging Challenges in Illinois Law Enforcement Collective Bargaining, Lewis Bender, Robert Fischer, and Thomas J. Jurkanin, January 2001.

Illinois Law Enforcement Executive Forum Journal, inaugural issue, June 2000.

Methamphetamine Labs: A New Danger for Illinois, 30-minute videotape, produced in cooperation with the U.S. Drug Enforcement Administration, Illinois State Police, through funds from the Illinois Law Enforcement Training and Standards Board.

Small Town Policing in the New Millennium: Strategies, Options, and Alternate Methods, Robin Johnson, author and researcher; published in cooperation with the Illinois Institute for Rural Affairs, March 2000.

Managing a Clandestine Laboratory Enforcement Program, Inspector Thomas McNamara, through a grant from the Illinois Law Enforcement Training and Standards Board, March 1999.

Model Domestic Violence Protocol for Law Enforcement, 1999, through a grant from the Illinois Criminal Justice Information Authority.

Making Empathy Statements to Defuse Conflict and Generate Rapport, Joseph Kulis et al., 1998.

Developing Persona Skills for Community Policing: A Manual for Trainers, Joseph Kulis, 1998.

An Assessment of Municipal and County Computer Crime Investigations in Chicago, Illinois Metropolitan Area, Bradley Byers, 1997.

Identifying the Future of Law Enforcement: 1997 Executive Forum Series Summary of Proceedings and Conference Notes, Illinois Law Enforcement Executive Institute in cooperation with the Illinois Law Enforcement Training and Standards Board, 1997.

Sex Crimes Investigation Course: Train-the-Trainer, Scott Keenan, Susan Welch, Polly Poskin, authors, Illinois Law Enforcement Executive Institute, 1997.

Police Executive's Perspectives of the Pre-Service Model, Kent Harrington, primary researcher and author, Illinois Law Enforcement Executive Institute, 1997.

Surviving and Thriving as a Law Enforcement Executive in the Twenty-First Century, May 1996, November 1996, June 1997, October 1997, June 1998.

Model Guidelines and Sex Crimes Investigation Manual for Illinois Law Enforcement, editor, Illinois Law Enforcement Executive Institute and the Illinois Coalition Against Sexual Assault through a grant from the Illinois Criminal Justice Information Authority, 1996.

Illinois Legislative Updates, 1995, 1996, 1997, Kevin Burke, author, Illinois Law Enforcement Executive Institute. (Videotapes produced as well as an annual satellite interactive television program through Educational Broadcasting at Western Illinois University.)

Zero Tolerance, 1994 Illinois Secretary of State Police. (Videotape produced as well as a satellite interactive television program through Educational Broadcasting at Western Illinois University.)

Sexual Assault Investigation Series (three tapes) in cooperation with the Illinois Coalition Against Domestic Violence through a grant from the Illinois Criminal Justice Information Authority, 1996.

1. *Preliminary and In-Depth Interview of the Victim of Adult Sexual Assault*
2. *Evidence Collection*
3. *Suspect Interview*

Domestic Violence Investigations Series (three tapes) in cooperation with the Illinois Coalition Against Domestic Violence and the Illinois Attorney General through a grant from the Illinois Criminal Justice Information Authority, 1997.

1. *Obvious Scenario*
2. *Subtle Scenario*
3. *Rural Scenario (Orders of Protection)*

Subscription to

Illinois Law Enforcement Executive Forum

Name _____

Organization _____

Address _____

City _____ State _____ Zip _____

Country _____

Subscription Categories for 2002-2003 only:

☐ Institutional – $40 ☐ Personal – $25

Enclosed is a check for $_____. Please add $20 for postage outside the U.S.

Subscription to

Illinois Law Enforcement Executive Forum

Name _____

Organization _____

Address _____

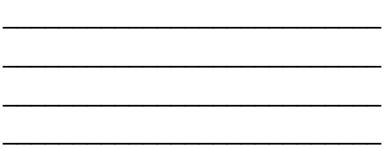
City _____ State _____ Zip _____

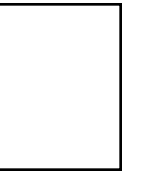
Country _____

Subscription Categories for 2002-2003 only:

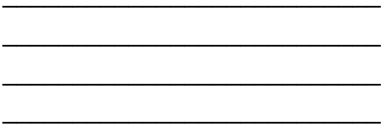
☐ Institutional – $40 ☐ Personal – $25

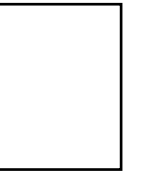
Enclosed is a check for $_____. Please add $20 for postage outside the U.S.





Illinois Law Enforcement
Executive Forum
1 University Circle
Macomb, IL 61455





Illinois Law Enforcement
Executive Forum
1 University Circle
Macomb, IL 61455